Alcatel-Lucent

8950 AAA (Authorization, Authentication, Accounting)
User's Guide | Release 6.0

365-360-001R6.0
ISSUE 1
DEC 2008

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners..

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2008 Alcatel-Lucent. All Rights Reserved.

Contents

About this information product

Overview

Purpose

Welcome, you are about to embark on a course to set up secure access to your network with the industry's leading RADIUS server, 8950 AAA. It provides you the highest level of control and management of a wide range of access services. These services range from simple dial-up remote access using Point-to-Point Protocol (PPP), Local Area Network (LAN) access, wireless (Wi-Fi) and wired, and even access to core network elements such as switches and routers.

RADIUS, or Remote Authentication Dial-In User Service, enables network operators to authenticate, authorize and account (AAA) for users. The RADIUS protocol defines communications between an access device or server and the RADIUS server. RADIUS-based security ensures that only users who meet your access criteria will be allowed access to a resource. The 8950 AAA server provides this functionality within an extensible, easy-to-use environment.

This manual introduces you to 8950 AAA through its friendly user interface, the Server Management Tool (SMT) and its integrated policy configuration tool, the PolicyAssistant. These tools provide a simple way to configure 8950 AAA for the most common AAA applications.

The PolicyAssistant creates, manages, and applies policies to control how and when users access your network. A policy is a set of rules that 8950 AAA uses to determine how users are authenticated, how access is authorized and configured, and how accounting data is stored.

The PolicyAssistant can be configured to support as many access policies as your network may require. You decide how many policies are necessary based on your business needs. These needs can include the type of services your network provides, your equipment requirements, your customers' requirements, or the geographic location of your customers.

Audience

This guide is designed to be used by qualified system administrators and network managers. Knowledge of basic networking concepts is required to successfully install 8950 AAA. You should be familiar with RADIUS server installation, configuration, and use.

Where to go First

How to Start

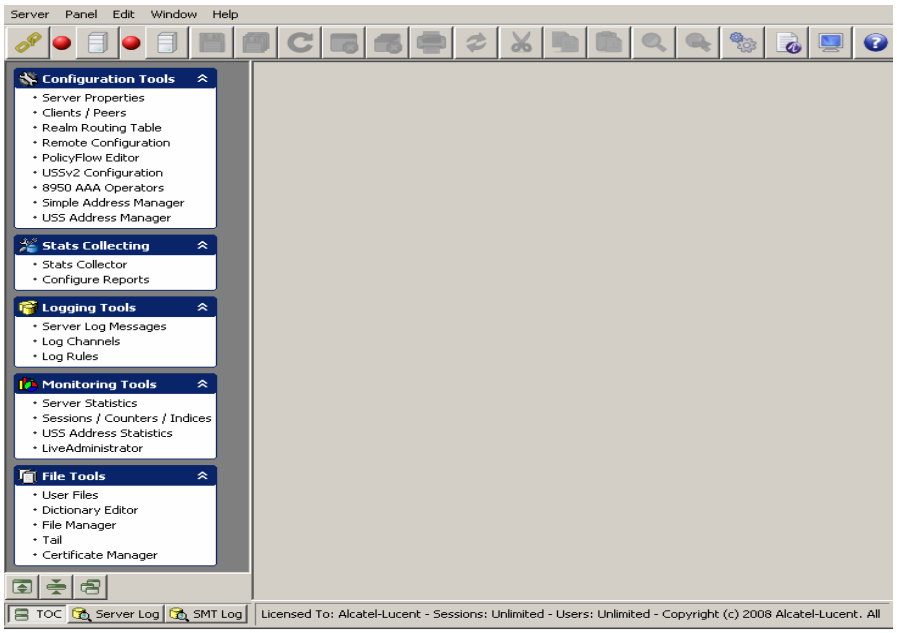
For more information about installing 8950 AAA and general software and hardware requirements, read the 8950 AAA *Quick Start Guide*.

If you are new to 8950 AAA, the links below should help determine where to go first:

Ready to configure 8950 AAA?

With the Server Management Tool (SMT) running, you should see the Policy Flow Editor in the Navigation pane as shown in Figure 1-1.

Figure 1-1 Server Management Tool-Navigation Screen



If you have already installed 8950 AAA and know how to launch the SMT, refer to the section "Using the Policy Wizard" on 9-4 to begin configuring your RADIUS environment.

Looking for the PolicyAssistant?

If you cannot find the PolicyAssistant in the Navigation pane when the Server Management Tool is running, refer to the section "Installing the PolicyAssistant and the Policy Flow Editor" on 3-13 to learn how to install the PolicyAssistant.

Attempting to start the Server Management Tool?

If you need help launching the Server Management Tool (SMT), refer to the section "Preparing to Create Your First Policy" on 9-3 to learn more about the SMT.

What is RADIUS?

If you are new to the RADIUS world of access control, refer to "RADIUS Terms Explained" on 1-3 to learn more about 8950 AAA and RADIUS terminology.

How This Manual Is Organized

Manual organization

This manual covers the steps necessary to set up your 8950 AAA server, clients, and user profiles to process user requests for network access. The manual is organized as follows:

Chapter 1, "Introduction to 8950 AAA"

This section provides an introduction to 8950 AAA and some of the terms that you will encounter when working with the 8950 AAA product.

Chapter 2, "8950 AAA Server Management Tool Overview"

This chapter covers the Server Management Tool layout and how to install the PolicyAssistant.

Chapter 3, "Server Management Tool Command Set"

This chapter discusses the Server Management Tool commands that are accessible from the menu bar, toolbar, and navigation pane of the user interface.

Chapter 4, "Managing 8950 AAA Servers"

This chapter addresses methods in controlling the behavior of 8950 AAA Servers.

Chapter 5, "Configuring 8950 AAA Client Properties"

This chapter discusses the process of configuring clients such as Network Access Servers (NASs) or other access points with the 8950 AAA SMT.

Chapter 6, “Configuring 8950 AAA Realm Routing Table Properties”

This chapter discusses the process of configuring the Realm Routing Table.

Chapter 7, “Configuring 8950 AAA Remotely”

This chapter discusses the process of configuring the 8950 AAA remotely.

Chapter 8, “Using the 8950 AAA Policy Flow Editor”

This chapter discusses the process of configuring and creating necessary entities for the Policy Flow Editor in the 8950 AAA Server Management Tool.

Chapter 9, “Using the 8950 AAA Policy Assistant in Server Management Tool”

This chapter discusses the process of how to use, configure, and create necessary entities for the PolicyAssistant in the 8950 AAA Server Management Tool.

Chapter 10, “Configuring 8950 AAA USSv2”

This chapter discusses the process of configuring the 8950 AAA USSv2 functionality.

Chapter 11, “Configuring 8950 AAA Operators”

This chapter provides information about defining administrator access to 8950 AAA. It defines different administrator roles and functions. It also provides information on how to use the SMT Operators panel.

Chapter 12, “Configuring Simple Address Manager”

This chapter discusses the tools that are used for the configuration and management of address pool by the Simple Address Manager. Simple Address Manager provides dynamic address pool management.

Chapter 13, “Configuring USS Address Manager”

This chapter discusses the tools that are available for the configuration and management of address pools of 8950 AAA, using Universal State server.

Chapter 14, “Stats Collector”

This chapter discusses about the various parts of 8950 AAA tool that collects statistical information of 8950 AAA.

Chapter 15, “Configuring Reports”

This chapter discusses about the reports configurator for the 8950 AAA tool.

Chapter 16, “Message Logging”

This chapter discusses how to determine the information that is logged, the format for logging it, and the destination for the logged information.

Chapter 17, “Server Statistics”

This chapter covers how to collect statistics for the 8950 AAA server.

Chapter 18, “Using LiveAdministrator”

This chapter discusses how to use the LiveAdministrator panel to manage, diagnose and control the 8950 AAA server.

Chapter 19, “Creating and Managing User Profiles with Files”

This chapter covers how to create a user file and add and edit user profiles.

Chapter 20, “8950 AAA Dictionary Editor”

This chapter provides information about the 8950 AAA Data Dictionary and some of the terms that you will encounter when working with the 8950 AAA product.

Chapter 21, “Managing files”

This chapter discusses 8950 AAA files and how to create and manage them using the File manager panel.

Chapter 22, “8950 AAA Certificate Manager”

This chapter discusses the 8950 AAA Certificate Manager, also known as *nrcert*. Root certificates generated with nrcert are *self-signed* certificates.

Chapter 23, “Creating and Managing User Profiles with the Built-in Database”

This chapter discusses how to manage user profiles stored in a Structured Query Language (SQL) database, besides managing database users, administrators, and 8950 AAA tables.

Chapter 24, “Server Diagnostics and Control Commands”

This chapter describes the 8950 AAA server control commands.

Appendix A, “Supplementary Information”

The appendix contains examples of 6 SMT text files that are produced through SMT activity.

Conventions

Table 1-1 lists the typographical conventions used throughout this manual.

Table 1-1 Conventions used in the document or manual

Convention	Meaning	Example
boldface	Names of items on screens. Names of commands, properties and plug-ins. Names of buttons you should click.	Click the **Enable** check box. The **AuthLocal** plug-in compares password attributes. Click **Validate** to check the syntax of the method.
Arial boldface	Names of keys you should press.	Press **Enter** to continue.
<angle brackets>	Variables that require you to substitute another value.	*http://<server IP address or name>* where <server IP address or name> is the address of name of the 8950 AAA server.
italics	Names of manuals or the first occurrence of a glossary term.	Refer to the 8950 AAA *6.0 User's Guide and Reference* for more information.
Arial italic	Directories, paths, file names, email addresses, and Uniform Resource Locators (URLs).	The 8950 AAA Web site is *http://www.8950AAA.com*
click	Press the left mouse button once.	To view the online help, click the book icon on the 8950 AAA toolbar.
right-click	Press the right mouse button once.	Right-click a Selector Type to view a list of selector types for method selection.
double-click	Press the left mouse button twice.	To open the Accounting Method Configuration panel, double-click anywhere on the tab display.

Recommended Reading

Reference reading

The following books cover a variety of topics that you might encounter while working with 8950 AAA. These books provide more information on the vast number of protocols and applications that 8950 AAA supports.

Building Internet Firewalls (2nd ed.). Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, and Deborah Russell. O'Reilly & Associates, Inc., 2000. (ISBN 1-56592-871-7)

Firewalls and Internet Security: Repelling the Wily Hacker (2nd ed.). William P. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. Addison-Wesley Publishing Company, February, 2003. (ISBN 0-20163-466-X)

Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architecture (4th ed.). Douglas E. Comer. Pearson Education, February, 2000. (ISBN 0-13018-380-6)

Mastering Regular Expressions (2nd ed.). Jeffrey E. F. Friedl. O'Reilly & Associates, Inc., July, 2002. (ISBN 0-59600-289-0)

RADIUS: Securing Public Access to Private Resources. Jonathan Hassell. O'Reilly & Associates, Inc., October, 2002. (ISBN 0-596-00289-6)

The DHCP Handbook (2nd ed.). Ralph E. Droms and Ted Lemon. Pearson Education, October 2002. (ISBN 0-67232-32 3)

Understanding PKI: Concepts, Standards, and Deployment Considerations (2nd ed.). Carlisle Adams and Steve Lloyd. Pearson Education, May 2002. (ISBN 0-67232-391-5)

Understanding and Deploying LDAP Directory Services (2nd ed.). Timothy A. Howes, Gordon S. Good, and Mark C. Smith. Addison-Wesley, May, 2003. (ISBN 1-67232-316-8)

UNIX in a Nutshell: A Desktop Quick Reference for SVR 4 and Solaris 7 (3rd ed.). Arnold Robbins. O'Reilly & Associates, Inc., August, 1999. (ISBN 1-56592-42 4)

Obtaining Technical Support

Technical Support

To contact Alcatel-Lucent for technical support, select the support channel that applies to you.

Support Channel 1: If you have purchased a 8950 AAA support contract, contact Alcatel-Lucent World-Wide Services (LWS):

- Customers in the USA and Canada, call 1-866-LUCENT8, Prompt 3. If you are not registered, use Prompt 7.
- Customers in other international locations, call +1-510-74 2000 or +1-410-381-3484
- Alcatel-Lucent Customer Support Web Site: *http://www.alcatel-lucent.com/support/*
- Alcatel-Lucent Customer Support Web Site: *http://support.lucent.com*

Support Channel 2: If you have purchased 8950 AAA within the last 90 days, you can contact Lucent Technologies World-Wide Services (LWS) for email support:

- Alcatel-Lucent Customer Support Web Site: *http://support.lucent.com*

Important! If you are a first time LWS support user OR if you have not yet registered your 8950 AAA service contract, contact LWS.

Support Channel 3: If you are evaluating 8950 AAA for purchase or need sales information or technical support (but do not have a support contract), contact us for:

- Technical support questions, review the 8950 AAA Discussion Forum: *http://www.8950AAA.com/cgi-bin/dcforum/dcboard.cgi*
- Pre-sales product questions, send an email to: *tech-sales@8950AAA.com*
- Sales information, send an email to *sales@8950AAA.com*
- Queries from Alcatel-Lucent employees, Sales Teams, VARS and Resellers, send an email to: *radius-internal@8950AAA.com*
- Other non-technical requests, send an email to: *tech-sales@8950AAA.com*

How to Comment

To comment on this information product, *Online(<http://www.lucent-info.com/comments>http://www.lucent-info.com/comments/)* email your comments to the Comments Hotline: comments@alcatel-lucent.com.

Part 1: Configuration Tools Navigation Pane

Overview

Purpose

This part consolidates the chapters related to Configuration Tools in the SMT Navigation pane.

Contents

This part includes the following chapters.

1 Introduction to 8950 AAA

Overview

Purpose

This chapter provides an introduction to 8950 AAA and some of the terms that you will encounter when working with the 8950 AAA product.

The following topics are included in this chapter:

What is 8950 AAA?

Overview

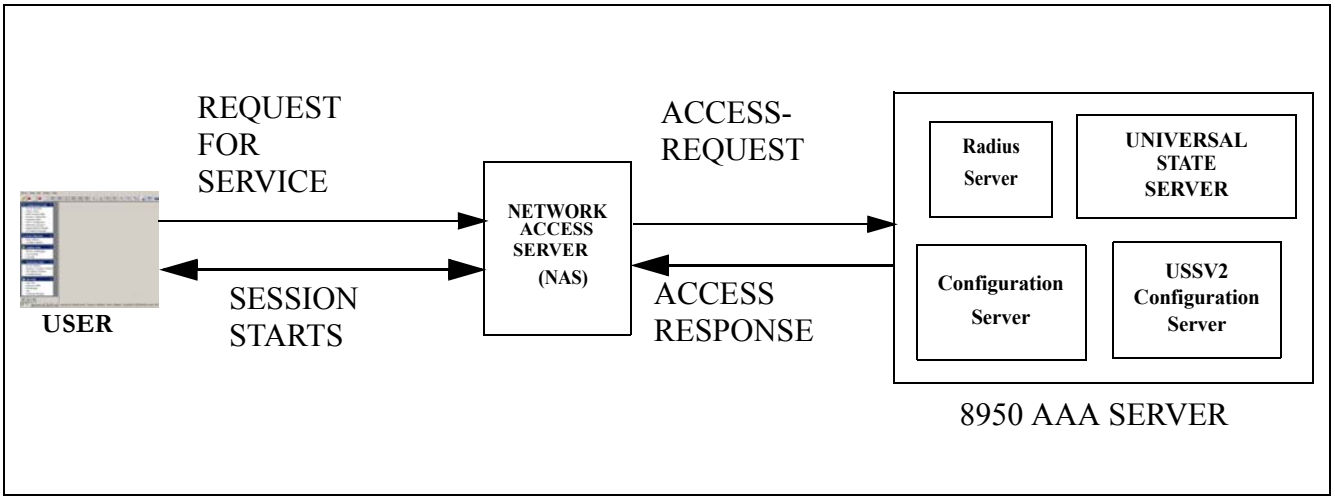
8950 AAA is server software that is used to manage secure access to networks, servers, and information services. Network elements that use a RADIUS server to manage access are known as clients. An example of a RADIUS client might be a network access server (NAS), a Wi-Fi access point, or even a Web page. 8950 AAA is a tool that promotes system integrity not only for the network server, but also for the client-server relationship.

The next section provides a scenario showing the role that 8950 AAA plays within a network.

Overview of Client-Server Access

8950 AAA provides access management for a client system. Figure 1-1 illustrates basically how this is done. The term *Network Access Server (NAS)* is a term for a network element that provides dial-up access services to a network. After the user connects to the NAS, the NAS receives the user name and password from the user's computer.

Figure 1-1 Accessing a Service



The NAS places this information into a RADIUS data packet called an *Access-Request*. This data packet identifies the NAS, the port used for connection, the user name, the password, and other information about the session.

The *Access-Request* is sent from the client to the server and asks the server if the user is allowed to use the requested services and access the network.

The process the server then follows may include the following actions, although none are required:

- Finding information about the user
- Validating the user's identity against information in a user profile
- Returning an answer (accept or reject) to the RADIUS client

A *user profile* contains information about a user that 8950 AAA uses to process a RADIUS request. The information usually includes the user name and password, and might include other information needed to implement local access policies. User profiles can be stored in files, databases, directories, Web-based services, etc. We call the location of the user profile the *user source*.

If local policy requirements are met then an authentication acknowledgement called an *Access-Accept*, is sent to the NAS along with other information defining specific settings for the user session. If local policy requirements are not matched, then the Access-Request is rejected by sending an *Access-Reject* message to the NAS.

RADIUS Terms Explained

Radius Overview

RADIUS is a client-server data communications *protocol*. The RADIUS protocol defines the types and contents of messages that can be exchanged in order to successfully access a system or service. The term RADIUS is an acronym that stands for Remote Authentication Dial-In User Services.

A RADIUS server is an example of an *authentication, authorization* and *accounting* (*AAA*-pronounced as “triple-A”) *server* because it authenticates a user, authorizes network access, records usage:

- *Authentication*–validating the user’s identity
- *Authorization*–validating that the user is allowed to do what was requested
- *Accounting* – recording information about a user’s session

The AAA environment is based on a client/server relationship. 8950 AAA implements the server functions and communicates with clients, such as Network Access Servers (NASs). The client is responsible for passing user information to RADIUS servers and acting on the response it receives. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and authorizing access, and then returning configuration information necessary for the client to deliver service to the user.

The RADIUS client controls the access protocols that are used. Within the protocol, *RADIUS Attributes* provide the vocabulary used for communication between RADIUS clients and servers. They provide authentication and authorization information, define session parameters, and record session accounting information. In the RADIUS protocol, attributes are defined by a number, a name, and a data type. For example, attribute number 1 is called User-Name and contains string, that is, character data. Each attribute contained in a RADIUS packet is assigned a value. For example, User-Name = Bob. This combination of an attribute name and an associated value is called an *Attribute Value Pair (AVP)*.

When configuring 8950 AAA, attributes are used in two ways: to return session settings to the client and to provide access check data in the authorization process. When used in these two ways, attributes are often called reply-items and check-items, respectively.

8950 AAA uses *policies* to define a set of rules that the server uses to determine access rights, user privileges, and accounting practices based on information contained in the Access-Request and information about the user who is requesting access. A *policy* defines the rules and steps the server follows to complete the process described above.

8950 AAA requires that at least one policy be defined, but it can be configured to handle many policies. You decide how many policies are necessary based on your business needs. The needs can range from the type and level of services you provide, equipment requirements, and customer requirements, to the geographic location of your customers and the time of day.

This document will describe use of the 8950 AAA *PolicyAssistant* to define access policies. It is also possible to create custom access policies using the 8950 AAA PolicyFlow programming language. Please refer to the 8950 AAA Programmer's Reference Manual.

Authentication and Authorization Activities

As mentioned previously, a *user source* is a data repository that contains user information called *user profiles*. 8950 AAA can access information stored in a variety of user sources. A user source might be one of the following:

- Standard text files, such as a RADIUS User file commonly used in publicly available RADIUS servers
- SQL databases, such as Oracle, Sybase, MySQL, or the built-in database
- An LDAP (Lightweight Directory Access Protocol) server or a server that supports LDAP queries, for example, Microsoft Active Directory or Novell NetWare directory

A user profile typically contains the user's name and password. Some user profiles may also contain information that describes the connection type, allowed services, authentication means, and session limits specific to a user.

The term *authentication source refers to the place where the user's authentication information, typically a password, is stored, for example, the user's profile,* or an external service that authenticates the user. An example of an external service is a secure token server.

Table 1-1 provides a list of supported sources for user profiles and a description of each. It is possible to read a user profile from one source and use a different source for authentication. For example, the user profile might be stored in LDAP while an RSA ACE (SecurID) might be used for authentication.

Table 1-1 Supported Sources for User Profiles

User Source	Description
RADIUS User File	A text file that conforms to a traditional format as used in many freeware RADIUS servers

User Source	Description
SQL Database	A database that accepts SQL (Structured Query Language) queries, for example, the built-in 8950 AAA database, and has a JDBC (Java Database Connectivity) driver
LDAP Directory	A directory service supporting LDAP (Lightweight Directory Access Protocol)
Microsoft Active Directory via LDAP	Directory service that is a part of Windows 2000, Windows XP, and Window 2003 Servers, using an LDAP interface.
Windows SAM	Windows Security Accounts Manager server that sits on top of the Windows 2000, Windows XP, and Window 2003 operating systems. This is only available when 8950 AAA is running on a Windows platform, local account, Windows domain, or Windows Active Directory.
UNIX System	When running on a supported UNIX or Linux system, 8950 AAA can retrieve user name and password information using the operating system.
Password File	8950 AAA can read the UNIX */etc/shadow* or */etc/passwd* files to access passwords for authentication.
ACE/Server	8950 AAA acts as a client for communicating with an RSA ACE/Server.
SafeWord	8950 AAA can communicate with a SafeWord server.
Proxy	8950 AAA can proxy (forward) data to another server that verifies the user name and password for authentication. It then waits for a response.

Accounting Activities

In addition, the 8950 AAA server can collect and store session and billing data. The server can save this data to text files (RADIUS Detail file), the built-in database, or any SQL database that supports a Java Database Connectivity (JDBC) driver, or forward the data to another RADIUS server.

END OF STEPS

2 8950 AAA Server Management Tool Overview

Overview

Purpose

This section describes how to utilize the 8950 AAA Server Management Tool. It contains information about how to start and how to navigate through the application. It describes the look and feel of the graphical user interface and lists the commands that are available to interact with 8950 AAA successfully.

The following topics are included in this chapter:

Purpose of the Server Management Tool

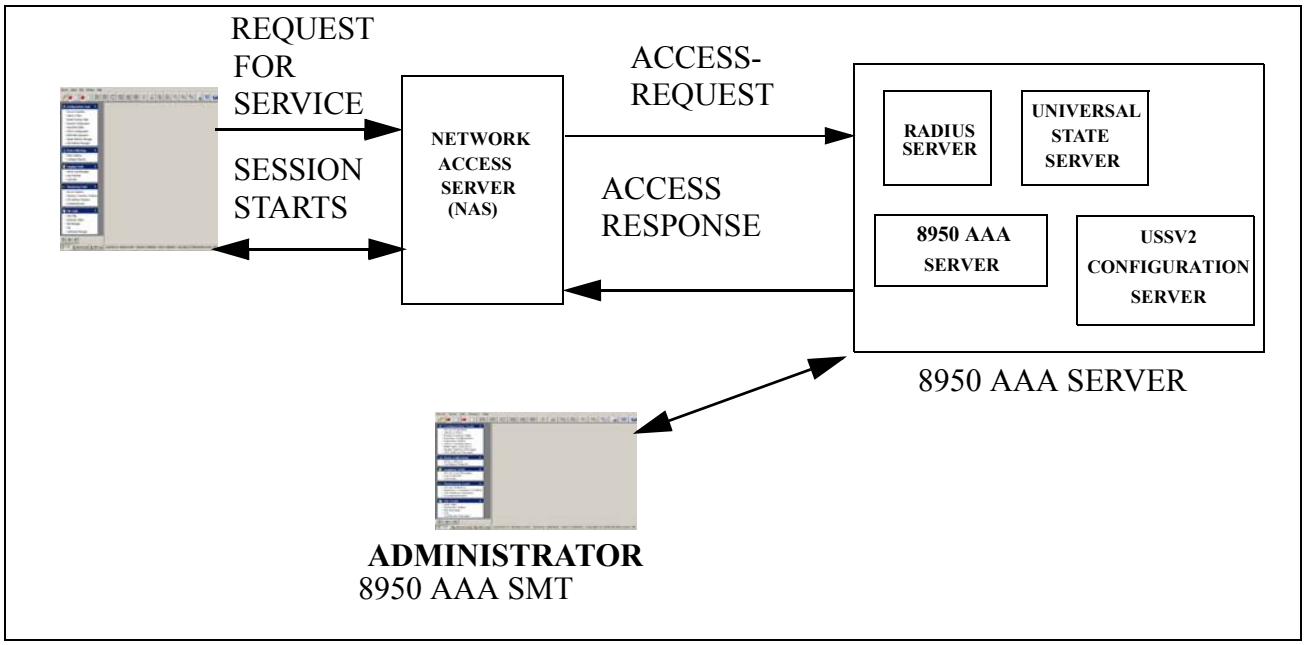
Overview

The 8950 AAA Server Management Tool (SMT) is an application that is used for configuring and managing 8950 AAA servers. It utilizes a graphical user interface or GUI that interfaces to the 8950 AAA server. It can be used to manage all aspects of server operation. The SMT also displays real-time statistical information from the RADIUS servers and Universal State Server (USS) systems.

The SMT is a standalone application that is started and run independently of the 8950 AAA server. The SMT may be run on the same computer as 8950 AAA or on a different computer. When the SMT is not run on the same platform as 8950 AAA then a small application called the 8950 AAA server must be started on the 8950 AAA platform before the SMT can be used.

Figure 2-1 illustrates the 8950 AAA SMT architecture.

Figure 2-1 8950 AAA System with SMT



The SMT contains a variety of tools including a menu bar, toolbar, navigation tools, and windows that provide the means to make server requests.

The following sections describe how to start the application and a basic overview of the GUI tools and commands.

Starting the Server Management Tool

How to start

To open the SMT, execute either of the following procedures:

1. On a Windows platform:

   From the Windows desktop, double-click the Server Management Tool icon/click the **Start** button to display the Start Menu. Select **Programs** to display the Programs Menu. Select **8950 AAA 6.0**. Click **Server Management Tool**.

   OR

   On a UNIX/Linux platform:

   Run the following command in the *bin* directory.

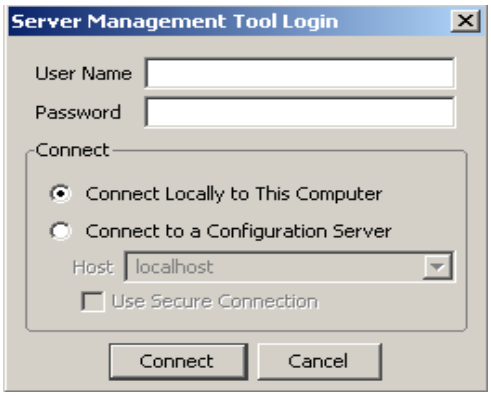
   `aaa-smt -u <user_name> -p <password>`

   For example, enter the following command line at the command prompt:

   `/AAA/bin/aaa-smt`

   Result: The 8950 AAA SMT Window opens and the login panel appears as shown in Figure 2-2.

Figure 2-2 SMT Login Panel



2. Enter the appropriate 8950 AAA **User Name** and **Password**.

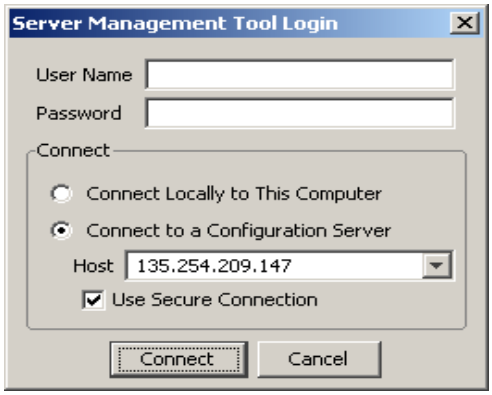
   Important! This can be an administrator name or a user configured for operator access.

3. Select the appropriate **Connect** option for your 8950 AAA server.

   You can open and edit files locally or connect to a remote 8950 AAA Server with the SMT.

   Result: When the SMT is not running on the same platform as the 8950 AAA server, the Configuration Server is used to execute commands issued by the SMT. In this case, the Configuration Server must be running on the 8950 AAA server. Enter the Host name or IP address to connect to a remote 8950 AAA server as shown in Figure 2-3.

Figure 2-3 SMT Login Panel-Connecting to Configuration Server



Important! Each instance of the SMT can only manage one 8950 AAA server at a time.

4. Choose the appropriate Host/IP address to connect to the appropriate 8950 AAA server.
5. Click **Connect** to connect to the mentioned host or 8950 AAA server.

Important! Appropriate certificates are installed during the initial installation of 8950 AAA server to use the Use Secure Connection option.

Important! Command to start the config server on Solaris is:

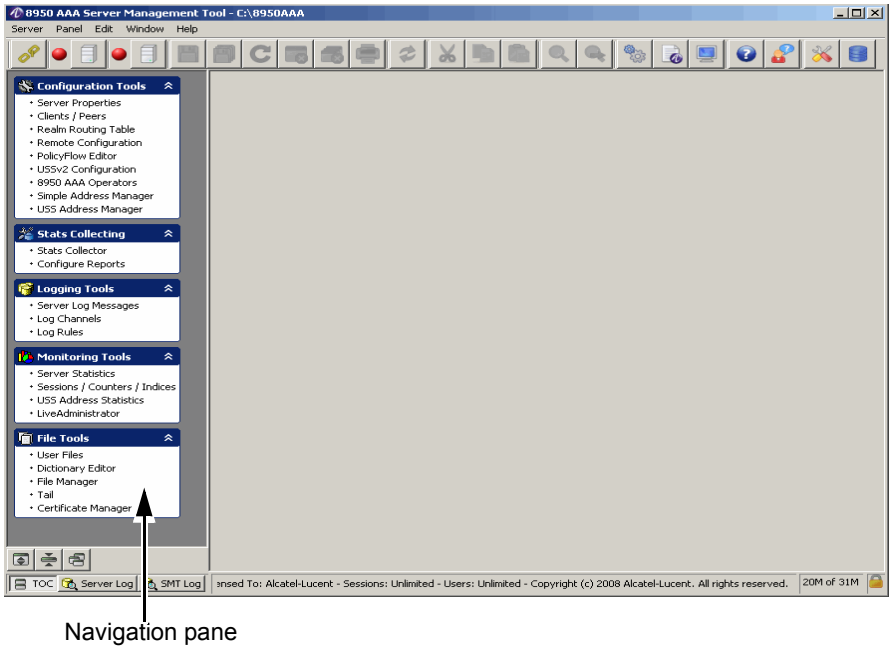
```
../bin/aaa start config
```

The Server Management Tool User Interface

SMT Interface

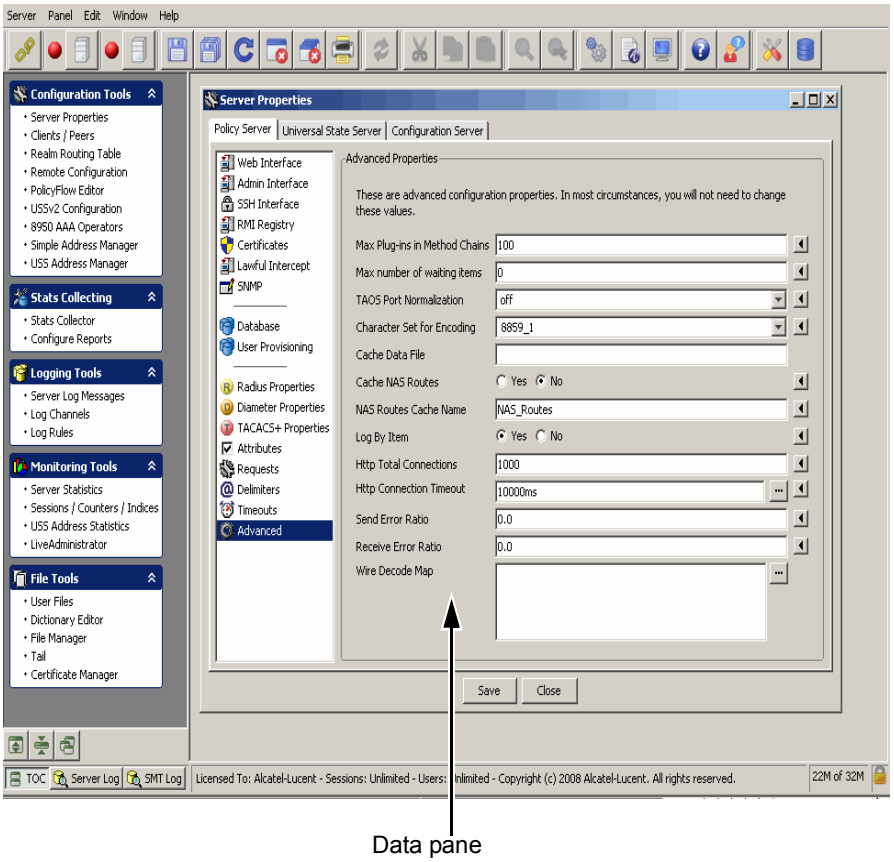
When you run the SMT, a window appears such as in the example in Figure 2-4. The following screen shows an example of the default screen.

Figure 2-4 The SMT User Interface-Default screen



The main frame of the window, located below the taskbar, is called the Data pane. The following screen shows an example of a Data pane when clicked on one of the menu options from the Navigation Pane.

Figure 2-5 SMT-Data Pane with example



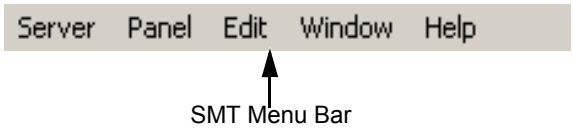
Important! A pane is a portion of a Window that behaves as a container. It can hold objects. A panel is a Window that can have GUI components such as tabs, text fields, buttons, and panes. Panels can be resized, minimized, and maximized within the SMT.

On the left side of the SMT window, beneath the toolbar, the Navigation pane lists 5 groups of configuration and management panels. If the user selects an item from the Navigation pane, a panel is displayed in the Data pane. The Data pane can display multiple panels simultaneously.

SMT Menu Bar

The 8950 AAA SMT menu bar appears at the top of the SMT interface as a list of menus as shown in Figure 2-6.

Figure 2-6 SMT-Menu Bar



Each menu contains a set of commands as described in Table 2-1.

Table 2-1 SMT Menu Commands

Menu/Command	Description
Server	
• Connect to Server	• Establish link to the 8950 AAA server.
• Disconnect from Server	• Log off from the currently connected 8950 AAA server.
• Exit	• Terminate the Server Management Tool.
Panel	
• Save Changes	• Save changes to the active panel.
• Revert to Last Saved	• Restore changes that have been saved for active panel.
• Reload Files	• Re-read modified 8950 AAA files into the running 8950 AAA server.
• Close	• Remove the active panel from the data pane.
• Print	• Send data from the active panel to the printer.
• Print Configuration	• Prints configurations with different print options.
Edit	
• Cut	• Copy selected information to the clipboard and delete the information.
• Copy	• Copy selected information to the clipboard.
• Paste	• Copy information from the clipboard to the selected location.
• Select All	• Indicate that all information from a source is to be acted upon.
• Find	• Search for information.
• Find Again	• Continue the last Find request.

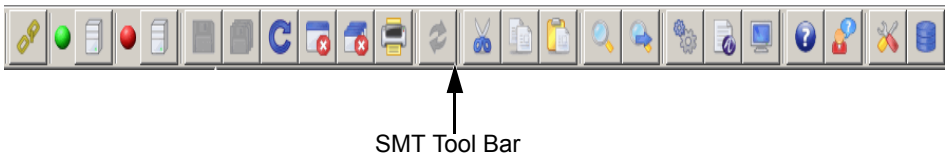
Table 2-1 SMT Menu Commands

Menu/Command	Description
• Preferences	• Customize SMT features for this and succeeding SMT sessions.
• Expand All	• Display all folder components within the navigation pane.
• Collapse All	• Display only folder names within the navigation pane.
Window	
• Cascade	• Display active panel followed other open panels using a stacked format with title bars in full view.
• Maximize	• Display a full view of the active panel. • Use the Next Window command to activate and display other open panels.
• Tile Horizontal	• Display a top-down list of all open panels.
• Tile Vertical	• Display all open panels from left to right.
• Arrange Icons	• Relocate panel icons to bottom of data pane.
• Next Window	• Activate next logical panel from pool of open panels.
• Save All	• Preserve data from all open panels.
• Close All	• Remove all open panels from data pane.
• Panel Names	• List of open panels in order of precedence.
Help	
• Help Contents	• Display general information within help pane.
• License Information	• Display license information.
• System Information	• Display system information.
• Support File Packager	• Display window for selecting information that requires support.
• About	• Display 8950 AAA release information.

SMT Toolbar

The SMT toolbar appears at the top of the SMT interface. It is a row of buttons as depicted in Figure 2-7.

Figure 2-7 SMT-Toolbar



The toolbar contains buttons that are used for executing commands within the application. The commands are described in Table 2-2.

Table 2-2 SMT Tool bar-Buttons

Buttons	Description
	Log off the currently connected 8950 AAA server. Use the connect menu option to reconnect.
	Show the status of the 8950 AAA Policy server running on the host of the currently connected 8950 AAA server. When the server is running, the button is green and if it is not running, the button is red. You can force a check by clicking the button.
	Provides Policy server management and allows control to the 8950 AAA Policy server. To manage the Policy Server, the following options are available: the name of the Policy Server, Start Server, Shutdown Server, Restart Server, Pause Server, and Resume Server.
	Show the status of the 8950 AAA Configuration server. When the server is running, the button is green and if it is not running, the button is red. You can force a check by clicking the button.
	Provides configuration server management and allows control to the 8950 AAA Configuration server. To manage the configuration Server, the following options are available: the name of the Configuration server, Start Server, Shutdown Server, and Restart Server.
	Save changes within the active panel. If no panel is displayed then this option is not available.
	Save changes in all displayed panels. If no panel is displayed then this option is not available.
	Revert to the last saved panel by abandoning changes to the active panel. The last saved panel is reloaded. If no panel is displayed then this option is not available. If no panel is displayed then this option is not available.

Table 2-2 SMT Tool bar-Buttons

	Close the active panel. If any changes have been made to that panel, a panel box appears asking if the changes should be saved. If no panel is displayed then this option is not available.
	Close all displayed panels. If changes have been made to any panel, a panel box appears asking if the changes should be saved. If no panel is displayed then this option is not available.
	Display a print panel box that provides print options for the user.
	Reload the files in the current panel for the 8950 AAA Servers.
	Copy selected information to the clipboard and delete the information.
	Copy selected information to the clipboard.
	Copy information from the clipboard to the selected location.
	Search for a text string that is specified within a panel box.
	Repeats the last search operation.
	Displays Configuration preferences.
	Displays License Information.

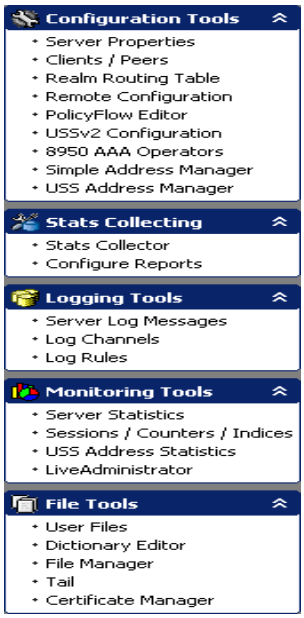
Table 2-2 SMT Tool bar-Buttons

	Displays System Information.
	Displays SMT help.
	Displays Technical Support File Packager window for gathering files and send to technical support.
	Allows you to launch test tools in another process.
	Allows you to launch database tools in another process.

SMT Navigation Pane

The Navigation pane is a list of panel names categorized according to the functionality, as shown in Figure 2-8.

Figure 2-8 SMT-Navigation Pane



There are 5 categories of panels or tools. The navigation pane can be linked to a toolbox because each panel provides a different tool and each tool can be accessed by selecting the panel name. The Navigation pane provides ease-of-use for the SMT user because it allows quick access to any of the listed panels.

Important! Your navigation pane may look slightly different depending upon the options you have installed and settings in your SMT preferences.

SMT Data Pane

The Data pane is the main area of the SMT window where panels are displayed. It is the gray area shown in Figure 2-9. Figure 2-10 shows the Data pane with a panel.

Figure 2-9 SMT-Data Pane without panels

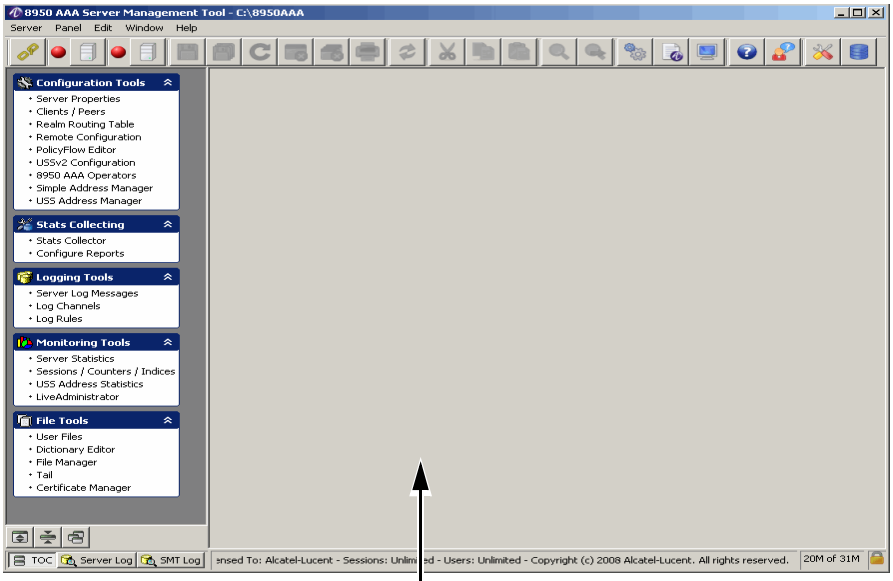
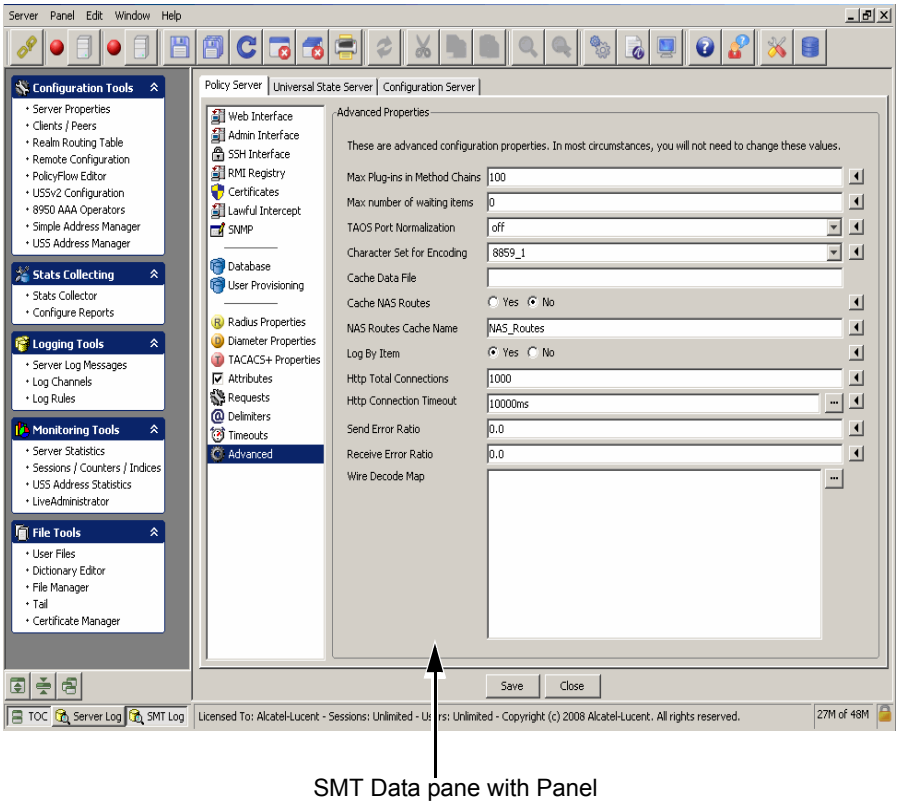


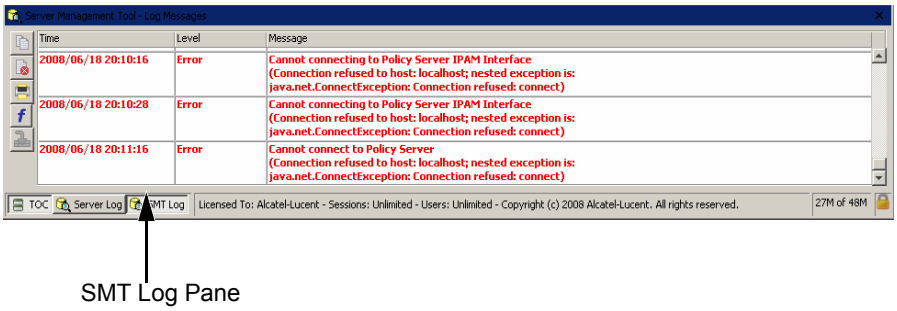
Figure 2-10 SMT-Data Pane with panel



SMT Log Pane

The Log pane appears at the bottom of the SMT user interface when you click on the SMT Log tab in the screen. The SMT Log pane is used for displaying log messages of the SMT, as shown in Figure 2-11.

Figure 2-11 SMT-SMT Log pane



The SMT Log pane contains buttons that are used for executing commands within the application. The commands are described in Table 2-3.

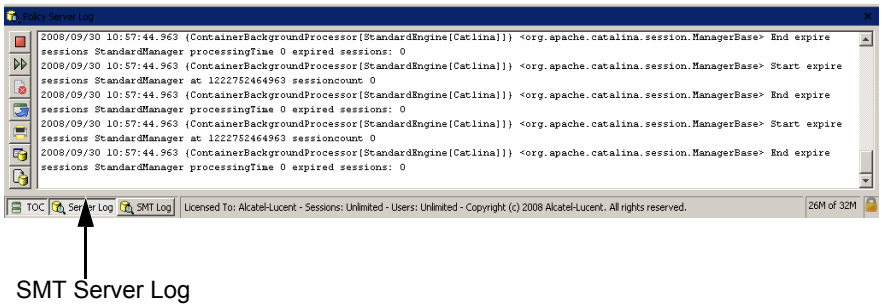
Table 2-3 SMT Log Pane–Buttons

Buttons	Description
	Copies the log information/message to clipboard.
	Clears the SMT Log pane.
	Prints the SMT Log pane information/message.
	Toggles the font in the SMT Log pane message table, from monspaced font to default font.
	Sets the log window to auto scroll. Displays the latest log message and scrolls the list of log messages as new messages are added.

SMT Server Log Pane

The Server log pane appears at the bottom of the SMT user interface when you click on the Server Log tab in the screen. The Server Log pane is used for displaying log messages from the server, as shown in Figure 2-12.

Figure 2-12 SMT-Server Log pane



The SMT server pane contains buttons that are used for executing commands within the application. The commands are described in Table 2-4.

Table 2-4 SMT Server Pane-Buttons

Buttons	Description
	Starts monitoring the Log files.
	To pause the monitoring process.
	Clears the SMT Server log pane.
	Opens the log file in a editor window.
	Prints the SMT Server pane information/message.
	Sets the log to the desired level.
	To select the desired log files from the list of log files displayed. Default is policy.log file.

END OF STEPS

3 Server Management Tool Command Set

Overview

Purpose

This section describes the SMT command set, focusing on commands that are found within the SMT menus. There is also information about panel commands and table management. The last section returns to the topic of the PolicyAssistant and lists a procedure on how to use the commands to install it.

The following topics are included in this chapter:

SMT menus and their commands

SMT Menus

As described in the section"SMT Menu Bar" on 2-6, the 8950 AAA Server Management Tool contains five command menus, as follows:

- Server
- Panel
- Edit
- Window
- Help

This section describes the commands in more detail.

Important! As discussed in Chapter 2, some SMT commands can be issued using the toolbar. Refer to the section"SMT Toolbar" on 2-8.

Server Connection

The *Server* menu contains commands that manage the connection between the SMT and the 8950 AAA server. It is found on the SMT menu bar. During the start procedure, either a local or remote connection to the configuration server is attempted. A local or remote connection is necessary to display and enable the SMT GUI.

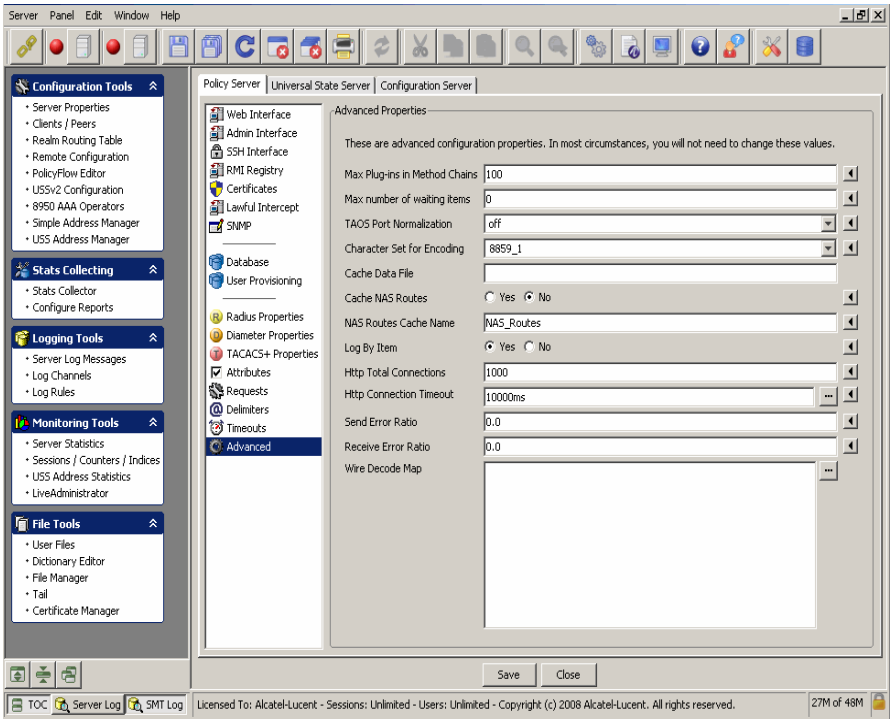
To break the connection to the 8950 AAA server, select **Server** on the menu bar and then click *Disconnect from Server.* As a result, the GUI disappears from the screen, except for the title bar and menu bar, and is replaced by the 8950 AAA logo icon.

To connect to a 8950 AAA server, select **Server** on the menu bar and then click *Connect to Server.* As during the start procedure, the Server Management Tool Login popup window appears so that the user can enter a username, password, and a mode of connection. After clicking **Connect**, the GUI appears again.

Managing Panels

The Server Management Tool uses panels to request or display information. Panels contain one or more tabs that have a variety of fields including text boxes, checkboxes, and drop-down lists. Some panels contain tables and graphs. Figure 3-1 shows an example of the SMT interface with a panel displayed.

Figure 3-1 SMT-Data pane with example panel

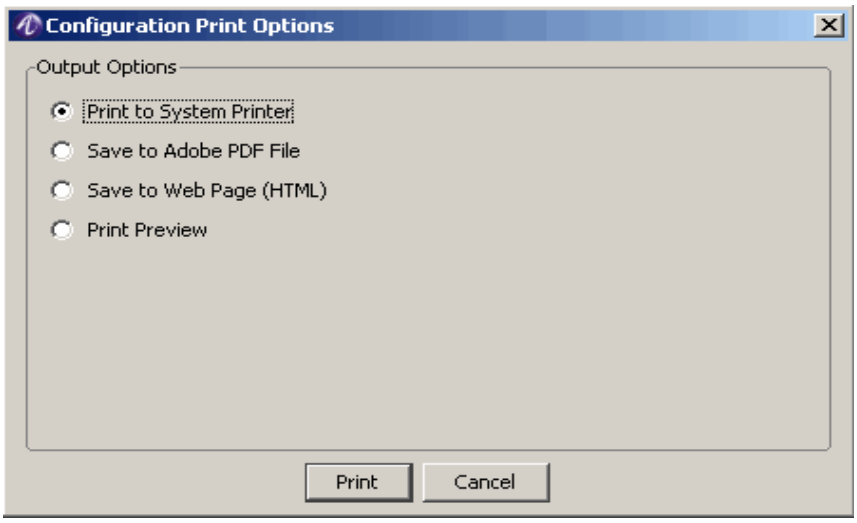


The *Panel* menu contains five commands that provide user control of the active panel. The active panel is the most recently displayed or selected panel within the SMT data pane. In most cases, the commands available on the *Panel* menu are also available as buttons on the panel itself and on the toolbar.

To display the *Panel* menu, select **Panel** on the menu bar. The following commands are available:

- The *Save Changes* command saves the most recent panel modifications.
- The *Revert to Last Saved* command restores active panel fields to values that were saved before any modifications were entered. If the modifications have been saved then this command will not restore the fields to any previous values.
- The *Reload Files* command provides the ability to reload modified versions of configuration files into the running 8950 AAA server.
- The 8950 AAA server loads certain files into memory when it is started, for example, the list of RADIUS clients. These files can also be reloaded while the server is running. If memory resident files are modified then they must be reloaded before the changes will take affect. The files must have been loaded at least once in order to use this command.
- The *Close* command closes the panel, removing it from the data pane.
- The *Print* command prints the contents of the active panel. If this command is selected then the **Configuration Print Options** panel is displayed, as shown in Figure 3-2.

Figure 3-2 Configuration Print options panel

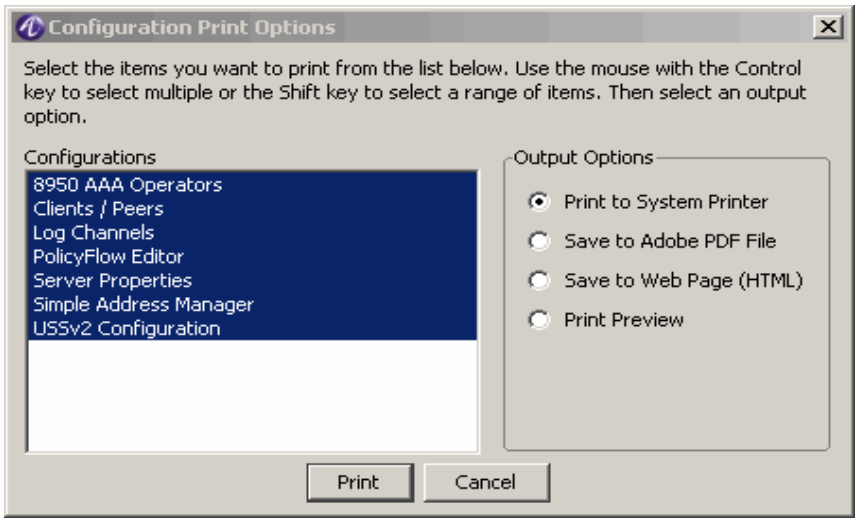


Select one of the available print options as described below:

- The *Print to System Printer* option sends the output to the default system printer.
- The *Save to Adobe PDF File* option saves the output to a PDF file created in the 8950 AAA *run* subdirectory.
- The *Save to Web Page (HTML)* option saves the output to an HTML file created in the 8950 AAA *run* subdirectory.
- The *Print Preview* option displays the output on the screen and provides an option to print it.

- The *Print Configuration* command option from the Panel menu displays a list of print configurations and helps to select the items that you want to print. If this command is selected then the **Configuration Print Options** dialog is displayed, as shown in Figure 3-3.

Figure 3-3 Configuration Print options dialog-Print Configuration option



Edit Commands

The *Edit* menu displays commonly used text editing commands as well as server preferences and data pane management options. To display the **Edit** menu, select **Edit** on the menu bar. Most of the commands on the **Edit** menu perform operations that are the same as with any GUI based application. The SMT Edit menu allows you to perform the *Cut, Copy, Paste, Select All, Find, Find Again, Preferences, Expand all, and Collapse all* commands.

Select *Preferences* to display the SMT Preferences panel, as shown in Figure 3-4.

Figure 3-4 SMT-Preferences Panel

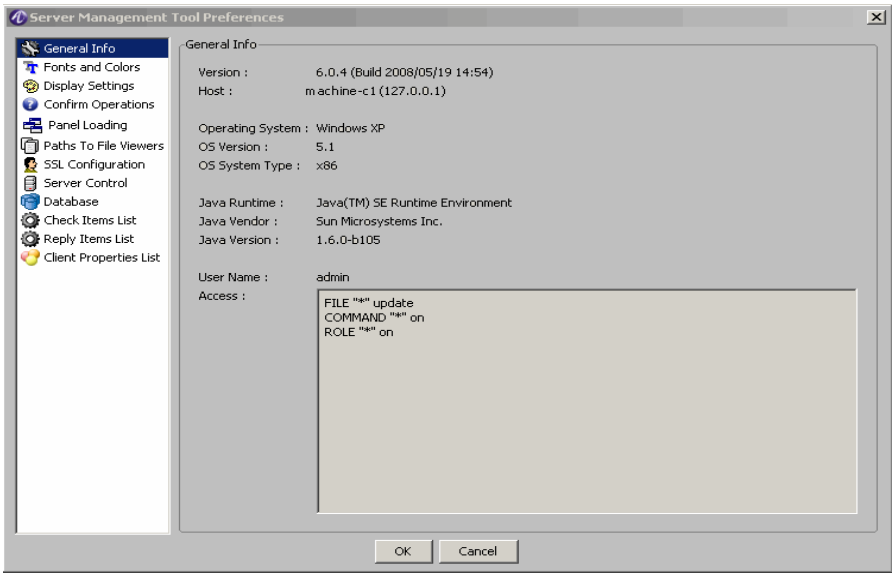


Table 3-1 describes the fields of the SMT Preferences Panel.

Table 3-1 SMT Preferences Panel-Properties

Configured Items	Description
General Info	Displays the general information such as Version details, Host Information, Operating System information, Java information, and so on.
Fonts and Colors	Controls display fonts, font size, and color schemes. UI Theme: Choice of color scheme used for SMT user interface appearance. Use System Fonts: Choose Yes to keep the default options. Choose No to edit the required options. Display Font: Choice of font used for SMT text display. Monospaced Font: Choice of font used for SMT logging and editing file input. Font Size: Choice of font size used for SMT text display. Use Antialised Font: Choose Yes to use the antialiased font and choose No to not choose this. Display Font Preview: Shows an example of selected display font and size. Monospaced Font Preview: Shows an example of selected monospaced font and size.

Table 3-1 SMT Preferences Panel-Properties

Configured Items	Description
Display Settings	Sets and display desktop components, icons, and windows sizes and locations. All the settings are Yes or No buttons. Choose appropriate buttons as per the requirement(s). Icons Show Icons in Resource Outline. Show Icons on Table Buttons. Shows Icons on Tabbed Panels. Windows Save Window Sizes and Location on Exit. Use Saved Window Sizes and Locations. Use Outline Dragging when Moving and Resizing Panels. Desktop Show Status Bar: Display the SMT status bar at the bottom of the main window. Used for displaying messages and errors. Show Tool Bar. Show Pop-up Tips.
Confirm Operations	Specifies the questions that are asked throughout the SMT. Confirm Server shutdown for the policy or configuration servers. All the settings are Yes or No buttons. Choose appropriate buttons as per the requirement(s).
Panel Loading	Specifies the panels to load in the Server Management Tool. Any changes to these properties will take effect next time you run the SMT. You can choose to load or not load all the available panels by selecting the Yes/No buttons that are provided next to each of the available panel names. All the settings are Yes or No buttons. Choose appropriate buttons as per the requirement(s).

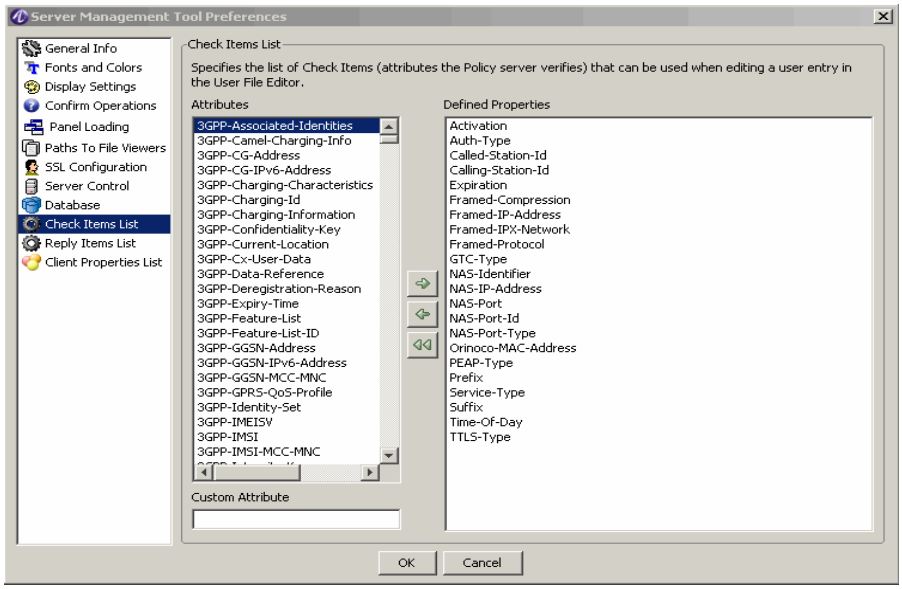
Table 3-1 SMT Preferences Panel-Properties

Configured Items	Description
Paths to File Viewers	Sets directory paths to Web browser, PDF viewer, and text file viewer. Web Browser Path: Indicates the location of the browser. PDF Viewer Path: Indicates the location of the application to view PDFs. Text File Viewer Path: Indicates the location of the application to view text files.
SSL Configuration	The SMT connects to the Configuration Server via RMI. Use the following to control whether the connections are secure (SSL). If you change this option, you must restart the SMT in order for it to take effect. Use secure remote connections when SMT in Local Mode: Choose Yes to use the secure remote connections when the SMT is in Local Mode. Choose No to not use the secure remote connections when SMT is in Local Mode. File for Trusted Certificates: Enter the filename that needs to be used for this.
Server Control	Sets how often the SMT checks the status of the 8950 AAA and configuration servers. On Windows platforms, controls 8950 AAA operation as a Windows service.
Database	Enables display of database panels and sets database connection options. Java JDBC Class: Specifies the Java JDBC Class file to use when connecting and for managing user records in your database. A database and a JDBC driver are included with your 8950 AAA server. JDBC Connection URL: Specifies JDBC connection URL. If you are connected to a database that is remote, replace localhost with the host name or IP address of the remote server.

Table 3-1 SMT Preferences Panel-Properties

Configured Items	Description
Check-items List	Sets the attributes displayed in the default Check-items list that is available in various SMT panels. You may select an attribute from the full dictionary attribute list, labeled **Attributes**, on the left side of the pane or enter your own attribute name in the custom attribute text box. Click the right arrow to add the attribute to the default list which appears in the window labeled **Defined Properties.**
Reply-items List	Sets the attributes displayed in the default Reply-items list that is available in various SMT panels. You may select an attribute from the full dictionary attribute list, labeled **Attributes**, on the left side of the pane or enter your own attribute name in the custom attribute text box. Click the right arrow to add the attribute to the default list which appears in the window labeled **Defined Properties.**
Client Properties List	Sets the properties displayed in the default Client Properties list that is available in various SMT Client settings panels. You may select an property from the full property list, labeled **Attributes**, on the left side of the pane or enter your own property name in the custom attribute text box. Click the right arrow to add the attribute to the default list which appears in the window labeled **Defined Properties**.

Figure 3-5 SMT Preferences Panel-Check-Items List

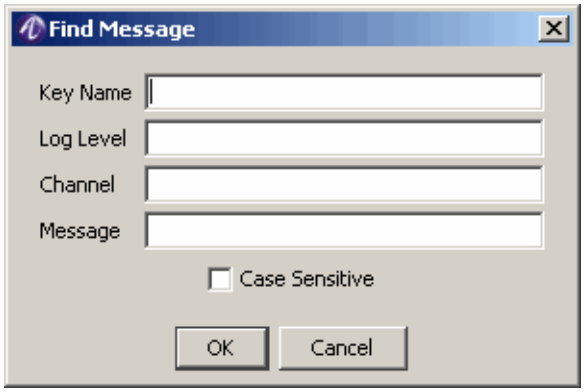


Search/Find

The Find Menu section has two options that helps to find or find once again the word/item you want to search.

- *Find*
- The find message screen is shown in Figure 3-6.
- *Find again*

Figure 3-6 Find Menu options



Other Edit Menu Commands

Under the Edit menu on the menu bar, the *Expand All* and *Collapse All* commands control the menus within the Navigation pane. By default, all menus are expanded in order to display all the panel names. To hide the panel names, select Collapse All.

Using the Window Menu to Manage Panels

This menu contains commands that allow the user to manage the panels that are open within the data pane. *Cascade, Maximize, Tile Horizontal, Tile Vertical,* and *Arrange Icons* display the panels as in other graphical user interfaces.

The *Maximize* command displays a full view of the active panel. Use the *Next Window* command to activate and display the next open panel. The *Next Window* command can also be used for cascaded panels. Alternatively, clicking the title bar of an open panel will activate it.

Each panel contains three window controls in the top right-hand corner of the panel, as shown in Figure 3-7.

Figure 3-7 Panel Control Buttons

They allow the user to minimize, maximize, and close the panel. A maximized panel will contain the **Restore** Windows control, as shown in Figure 3-8.

Figure 3-8 Panel Restore Button

Clicking this control resizes the panel to its previous form.

Minimizing a panel converts it to an icon. The *Arrange Icons* command allows the user to move all panel icons to the bottom of the data pane. Double-click a minimized icon to restore it to its previous size.

The *Save All* command saves the contents of all open panels to the database. The *Close All* command removes all panels from the data pane.

The **Window** menu contains a numbered list of all open panels in order of precedence. The active panel is always first in the list. Click the name of an open panel in the list to activate it and make it first in the list.

Managing Data in SMT Panels

About managing data in SMT panel

The SMT uses graphical panels to allow you to easily view, add, change, edit and remove configuration items. While each of these panels is designed to manage specific data types (Clients, Attributes, Realms, Users, etc.) they share many common control functions.

Table 3-2 describes six of the most common panel control functions.

Important! In some cases more than one icon may be used for a given function. This is due to space limitations on some of the panels.

Table 3-2 Panel Control Functions

Action	Description	Button Icon
Insert	Add a record in the current panel after the selected row. If no row is selected, the record is inserted at the end of the table or list. Clicking this button typically displays a panel to enter information.	
Edit	Edit data for an existing record. Clicking this button typically displays a panel to enter information.	
Delete	Remove the selected row from the current panel's table.	
Delete All	Remove all records from the current panel.	
Make a Copy of selected record	Duplicate the selected record. The duplicate record is inserted after the selected record.	 
Row Order	Some panels contain order sensitive data. When using these panels, you may change the order of records by selecting a record and then using the Up-Down buttons as appropriate.	  

Sizing Table Columns

Resizing the table columns

You can resize columns in a table. To resize a column, pass the mouse over the line dividing the table columns in the title row, that is, the top row of the table where the column names appear. The mouse changes to a resize pointer. Click and drag in either direction. If a column is too narrow to display a table entry, a small arrowhead appears to indicate that data has been truncated.

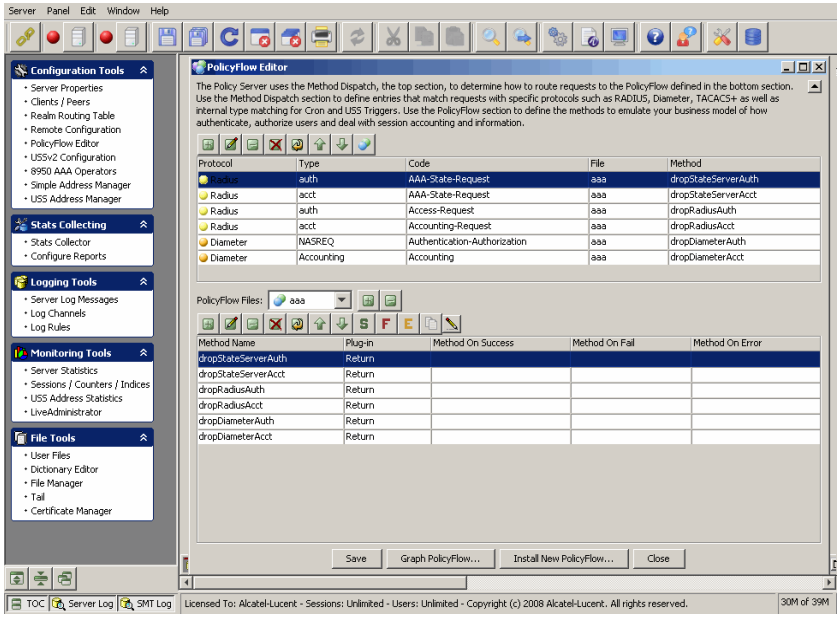
Installing the PolicyAssistant and the Policy Flow Editor

Installing PolicyAssistant

You can choose to install and work on either the Policy Flow Editor or the Policy Assistant at a time. By default, the Policy Flow Editor is enabled when you install the 8950 AAA GUI. To enable the Policy Assistant, perform the following steps.

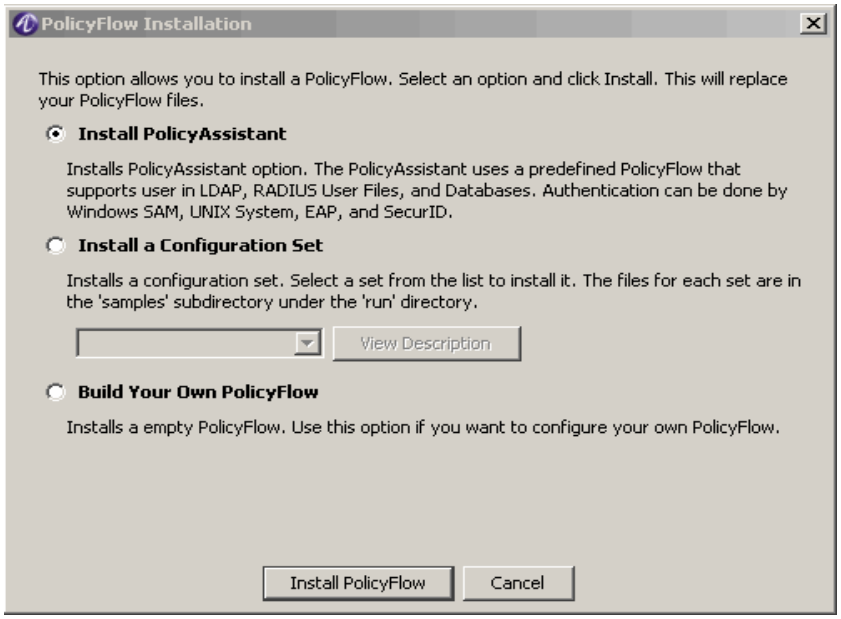
1. Select **Policy Flow Editor** from the Navigation pane under the Configuration Tools section. The **Policy Flow Editor panel** is displayed as shown in Figure 3-9.

Figure 3-9 SMT-Policy Flow Editor Panel



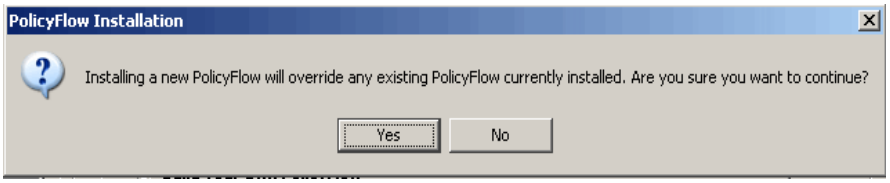
2. Click the **Install PolicyFlow...** to open the **PolicyFlow Installation** page. The **PolicyFlow Installation** page is displayed as shown in Figure 3-10.

Figure 3-10 SMT-Policy Flow Installation page



3. Select **Install Policy Assistant** and click the **Install Policy Flow** button. The following message appears.

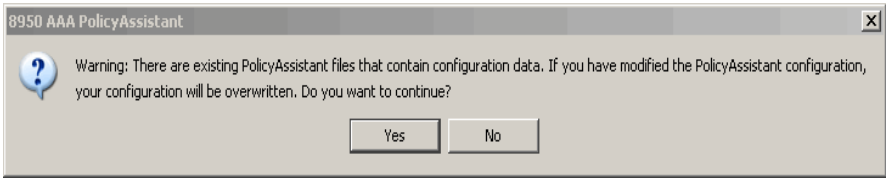
Figure 3-11 SMT-Policy Flow Installation warning message



4. Click **Yes** to continue.

   Important! If the Policy Flow Assistant is already installed, the following message appears.

Figure 3-12 SMT-Policy Flow warning message



5. Click **Yes** to continue. It will take a few seconds and when the installation is complete, the following message appears.

Figure 3-13 SMT-Policy Flow Installation success message

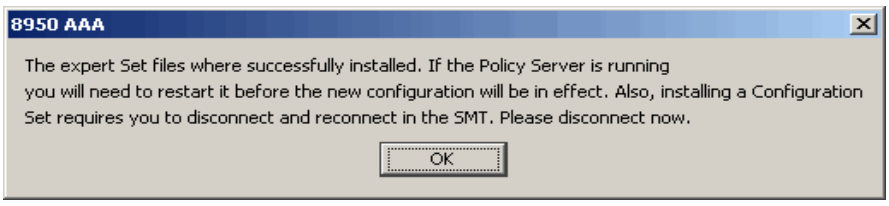
6. Click OK and close the SMT GUI and restart the application.
7. After you restart, instead of the **PolicyFlow Editor**, you will see the entry **Policy Assistant** in the Navigation pane under the Configuration Tools section.

Read through Chapter 9, "Using the 8950 AAA Policy Assistant in Server Management Tool" for more information on the PolicyAssistant. While the PolicyAssistant is very easy to use, there are some decisions you must make to successfully set up 8950 AAA.

Installing PolicyFlow Editor

1. To enable the PolicyFlow Editor, perform the following steps:
2. In the PolicyAssistant panel, click **Install PolicyFlow..** to open the **PolicyFlow Installation** page. The **PolicyFlow Installation** page is displayed as shown in Figure 3-10.
3. Select **Build Your Own PolicyFlow** and click the **Install Policy Flow** button. A warning message, as shown Figure 3-11 appears.
4. Click **Yes** to continue.
5. If the Policy Flow Editor is already installed, one more warning message as shown Figure 3-12 appears.
6. Click **Yes** to continue. It will take a few seconds and when the installation is complete, the following message appears.

Figure 3-14 SMT-Policy Flow Installation success message



7. Click OK and close the SMT GUI and restart the application.
8. Once you restart, you will see that instead of the **Policy Assistant**, you will see the entry **Policy Flow Editor** in the Navigation pane under the Configuration Tools section.

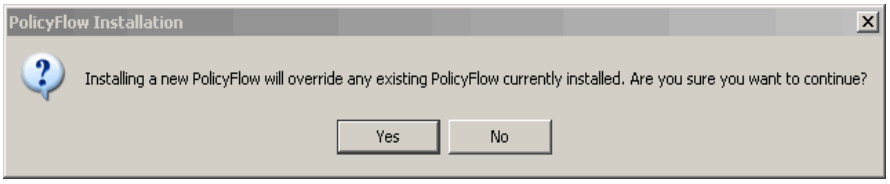
Read through Chapter 8, "Using the 8950 AAA Policy Flow Editor" for more information on the PolicyFlow Editor.

Installing PolicyFlow Editor for a configuration set

To enable the PolicyFlow Editor for a configuration set, perform the following steps:

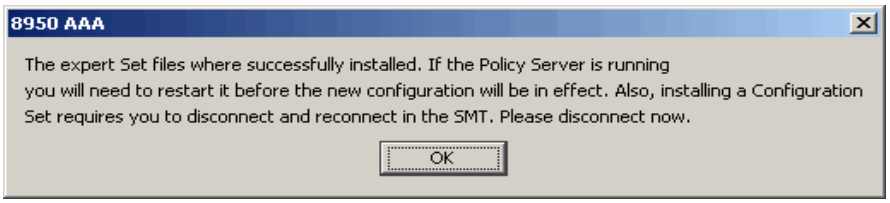
1. In the **PolicyFlow Installation** page, as shown in Figure 3-10, select **Install a Configuration Set.**
2. The drop-down list box is activated and this shows a list of pre-configured configuration sets.
3. Select one of the configuration set from the list and click the **Install Policy Flow** button. A warning message, as shown Figure 3-15 appears.

Figure 3-15 SMT-Policy Flow-already existing warning message



4. Click **Yes** to continue. It will take a few seconds and when the installation is complete, the following message appears.

Figure 3-16 SMT-Policy Flow Installation success message



5. Click OK and close the SMT GUI and restart the application.
6. Once you restart, you will see that instead of the **Policy Assistant**, you will see the entry **Policy Flow Editor** in the Navigation pane under the Configuration Tools section.

   Important! If you click on the **Policy Flow Editor** in the Navigation pane, the SMT will display the configuration set that was selected in step 2.

END OF STEPS

4 Managing 8950 AAA Servers

Overview

Purpose

This section discusses how the SMT is used to control the behavior of 8950 AAA servers and to define properties associated with the servers.

The following topics are included in this chapter:

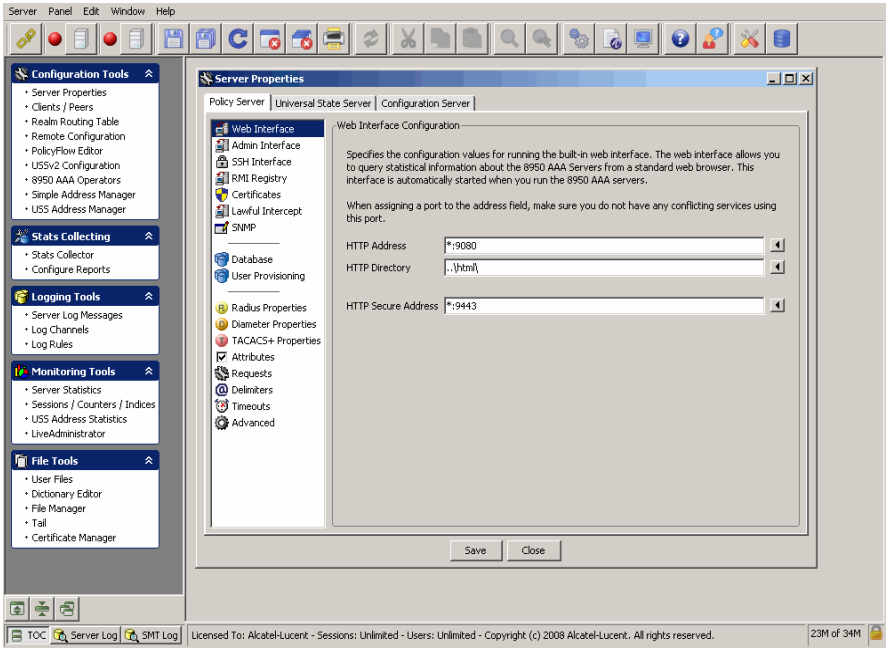
Configuring Server Properties

About Configuring the Server properties

Before 8950 AAA can start processing AAA (“triple-A”) traffic, it must first be configured for your local environment and specific policy needs. 8950 AAA allows the user to control the behavior of the 8950 AAA RADIUS server by setting configuration options. The various configuration options control how 8950 AAA servers process packets and manage data flow.

The configuration options are provided within the Server Properties Panel. To open this panel, locate Configuration Tools within the SMT Navigation Pane and select **Server Properties**. The Server Properties Panel appears as shown in Figure 4-1.

Figure 4-1 Server Properties Panel



The Server Properties Panel

Use the Server Properties panel to control the behavior of the 8950 AAA servers including how the 8950 AAA server processes packets and manages data flow between its servers and clients.

The Server properties panel display 3 tabs as follows:

- Policy Server
- Universal State Server
- Configuration Server

Each of these tabs allow you to configure different types of interface.

Policy Server tab

About the Policy Server tab

The Policy Server tab allows you to configure the entities in the policy server.

By default, when you click on the Server Properties option, the Policy Server tab is displayed. In the Policy Server tab, by default, the **Web Interface Configuration** panel is displayed as shown in Figure 4-1.

Web Interface Configuration Panel

The Web Interface Configuration panel specifies the configuration values for running the built-in web interface. The web interface allows you to query statistical information about the 8950 AAA servers from a standard web browser. This interface is automatically started when you run the 8950 AAA servers.

> **Important!** When assigning a port to the address field, make sure you do not have any conflicting services using this port.

Table 4-1 lists the configurable entities of this panel.

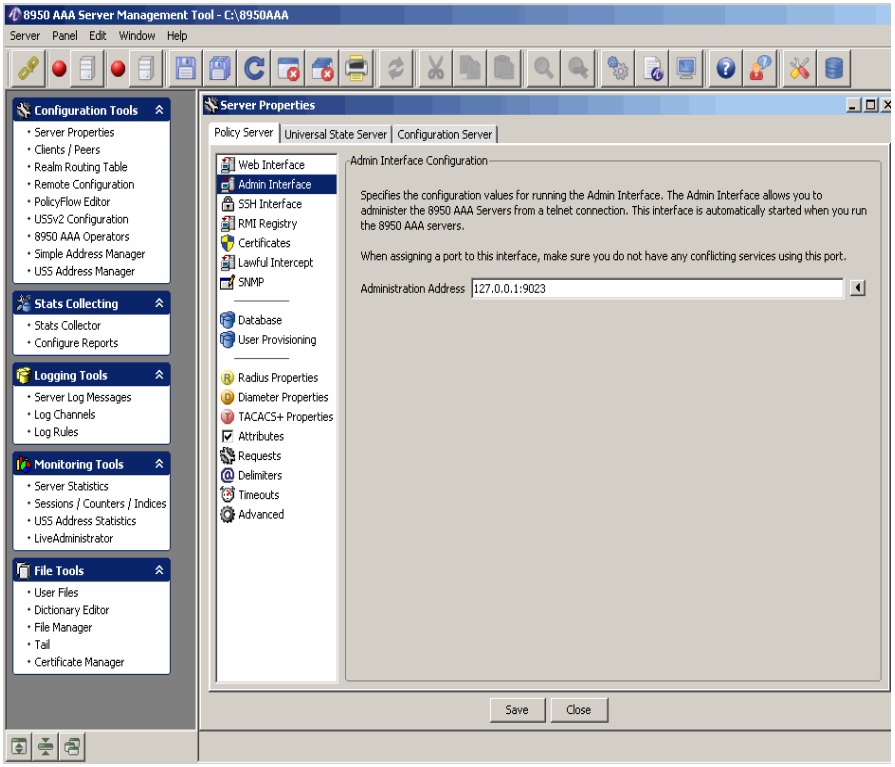
Table 4-1 Policy Server Tab-Configurable properties

Configurable Properties	Description
HTTP Address	Sets the address for the HTTP connection to the built-in web interface. Default is '*:9080'.
HTTP Directory	Specifies the root directory where the server looks for its HTML files used by its web server. If a full path is not included, this filename is relative to the run directory. Default is '..\html\'.
HTTP Secure Address	Sets the address for secure (HTTPS) HTTP connection to the built-in web interface. Default is '*:9443'.

Admin Interface Configuration Panel

To go to the Admin Interface Configuration panel, click on the **Admin Interface** option from the Policy Server data pane menu options on the left side. The Admin Interface Configuration panel is displayed as shown in Figure 4-2.

Figure 4-2 Policy Server-Admin Interface Configuration Panel



The Admin Interface Configuration panel specifies the configuration values for running the Admin interface. The Admin interface allows you to administer the 8950 AAA servers from a telnet connection. This interface is automatically started when you run the 8950 AAA servers.

Important! When assigning a port to this interface, make sure you do not have any conflicting services using this port.

Table 4-2 lists the configurable entities of this panel.

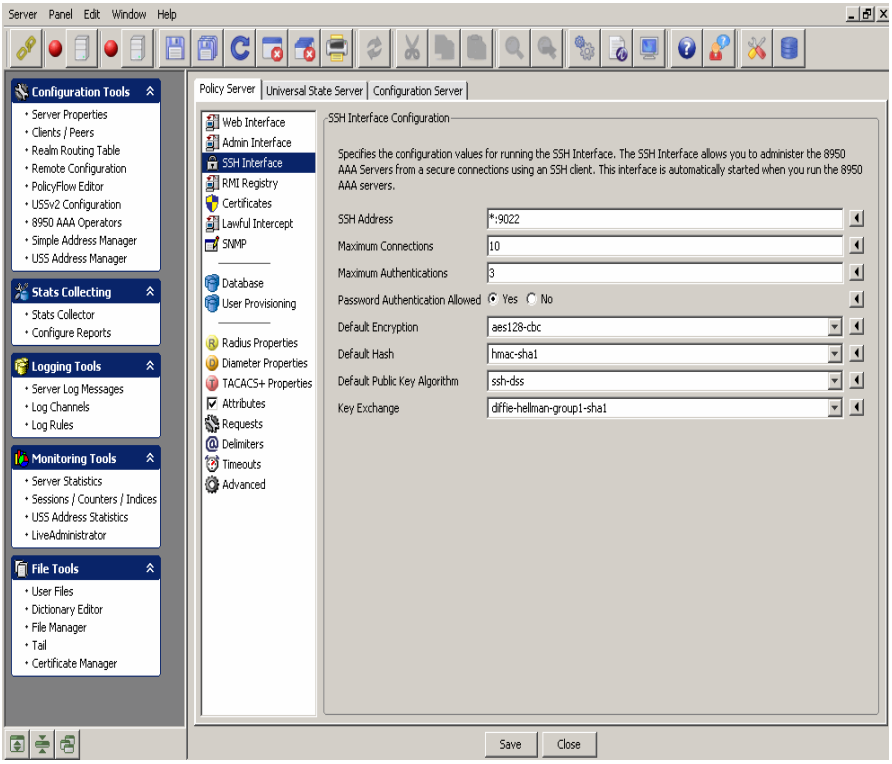
Table 4-2 Admin Interface Configuration panel-properties

Configurable Properties	Description
Administration Address	Sets the address for telnet connections to the built-in admin interface. Default is ‘127.0.0.1:9023’.

SSH Interface Configuration Panel

To go to the SSH Interface Configuration panel, click on the **SSH Interface** option from the Policy Server data pane menu options on the left side. The SSH Interface Configuration panel is displayed as shown in Figure 4-3.

Figure 4-3 Policy Server-SSH Interface Configuration Panel



The SSH Interface Configuration panel specifies the configuration values for running the SSH interface. The SSH interface allows you to administer the 8950 AAA servers from secure connections using an SSH client. This interface is automatically started when you run the 8950 AAA servers.

Table 4-3 lists the configurable entities of this panel.

Table 4-3 SSH Interface-Properties

Configurable Properties	Description
SSH Address	Specifies the address and port the server listens to, default is '*:9022' and port number 0 means do not start the SSH at all.
Maximum Connections	Specifies the maximum number of simultaneous connections against the SSH server at any given time. Entering a value of 0 disables the SSH Service.
Maximum Authentications	Specifies the maximum number of unsuccessful authentication attempts in a row that a user is permitted before being kicked off.
Password Authentication Allowed	Specifies that the password authentication is allowed. Password forces a standard username and password login.

Table 4-3 SSH Interface-Properties

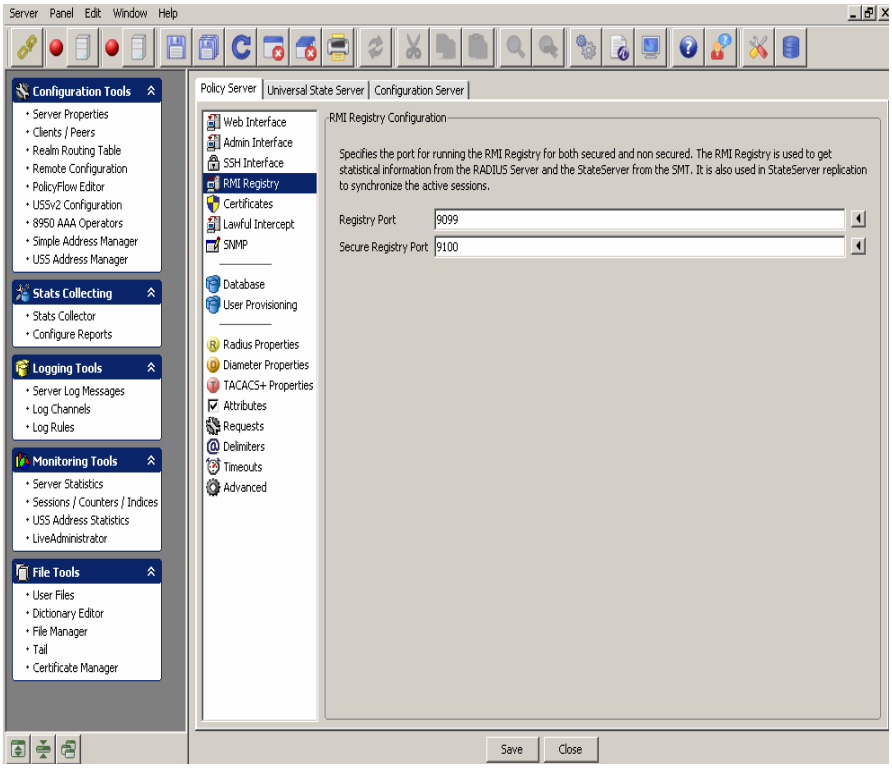
Configurable Properties	Description
Default Encryption	Specifies the default encryption to use for connections if not specified by the client.
Default Hash	Specifies the default hash algorithm to use for connections if not specified by the client.
Default Public Key Algorithm	Specifies the default public key algorithm to use for connections if not specified by the client.
Key Exchange	Specifies the key exchange configuration. Currently only ‘diffie-hellman-group1-sha1’ is supported.

RMI Registry Configuration Panel

The Remote Method Invocation (RMI) Registry property is used to set the port for running the RMI Registry. The panel contains one field that contains the Registry Port that the server uses for accepting connections from the SMT for retrieving statistical information about statistics, counters, indices, and port status. This port is used to replicate data between the primary and secondary state servers.

To go to the RMI Registry Configuration panel, click on the **RMI Registry** option from the Policy Server data pane menu options on the left side. The RMI Registry Configuration panel is displayed as shown in Figure 4-4.

Figure 4-4 Policy Server-RMI Registry Configuration Panel



The RMI Registry Configuration panel specifies the port for running the RMI Registry for both secured and non secured. The RMI Registry is used to get statistical information from the RADIUS Server and the StateServer from the SMT. It is also used in StateServer replication to synchronize the active sessions.

Table 4-4 lists the configurable entities of this panel.

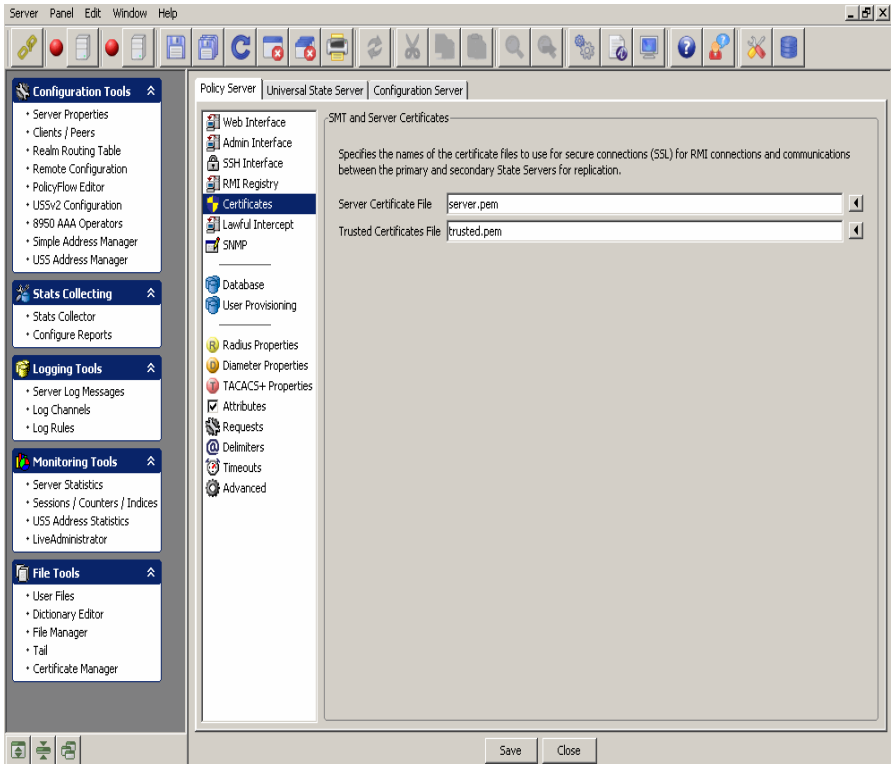
Table 4-4 RMI Registry-Properties

Configurable Properties	Description
Registry Port	Specifies the Registry Port the server uses for accepting connections from the SMT to retrieve statistical information about statistics, counters, indexes, and port status. This port is used to replicate data between the primary and secondary state servers. Default value is ‘9099’.
Secure Registry Port	Same as Registry Port. Default value is ‘9100’.

SMT and Server Certificates Panel

To go to the SMT and Server Certificates panel, click on the **Certificates** option from the Policy Server data pane menu options on the left side. The SMT and Server Certificates Configuration panel is displayed as shown in Figure 4-5.

Figure 4-5 Policy Server-SMT and Server Certificates Panel



The SMT and Server Certificates panel specifies the names of the certificate files to use for secure connections (SSL) for RMI connections and communications between the primary and secondary state servers for replication.

Table 4-5 lists the configurable entities of this panel.

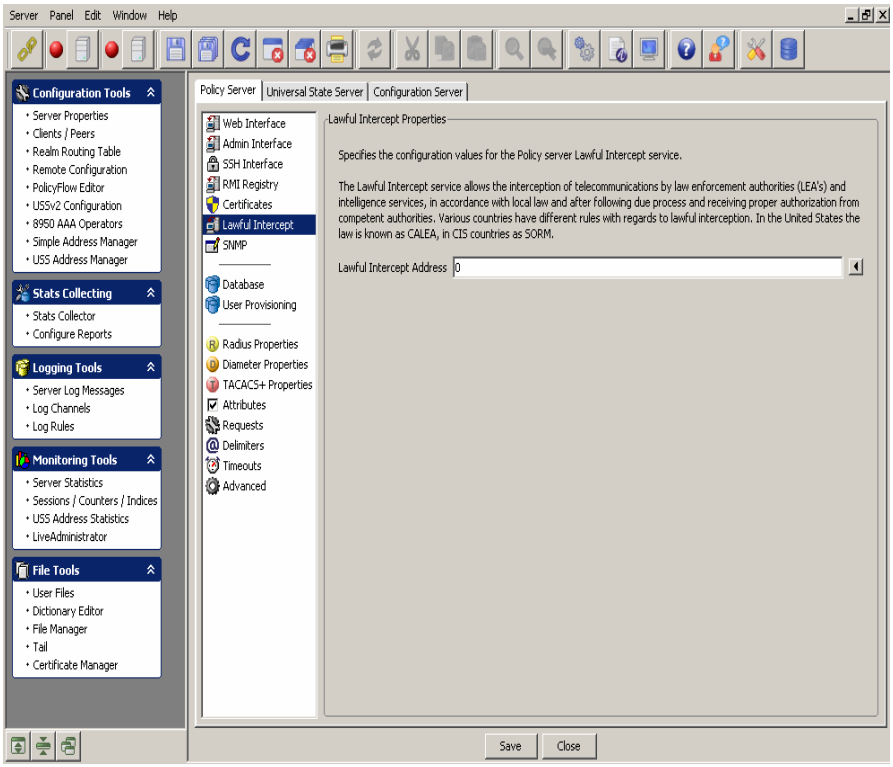
Table 4-5 SMT and Server Certificates panel-Properties

Configurable Properties	Description
Server Certificate File	The server certificate file. Default file is ‘server.pem’.
Trusted Certificates File	The trusted certificates file. Default file is ‘trusted.pem’.

Lawful Intercept Properties Panel

To go to the Lawful Intercept Properties panel, click on the **Lawful Intercept** option from the Policy Server data pane menu options on the left side. The Lawful Intercept Properties panel is displayed as shown in Figure 4-6.

Figure 4-6 Policy Server-Lawful Intercept Properties Panel



The Lawful Intercept Properties panel specifies the configuration values for the policy server lawful intercept service.

The Lawful Intercept service allows the interception of telecommunications by law enforcement authorities (LEA's) and intelligence services, in accordance with local law and after following due process and receiving proper authorization from competent authorities. Various countries have different rules with regards to lawful interception. In the United states the law is known as CALEA, in CIS countries as SORM.

Table 4-6 lists the configurable entities of this panel.

Table 4-6 Lawful Intercept Properties Panel-Properties

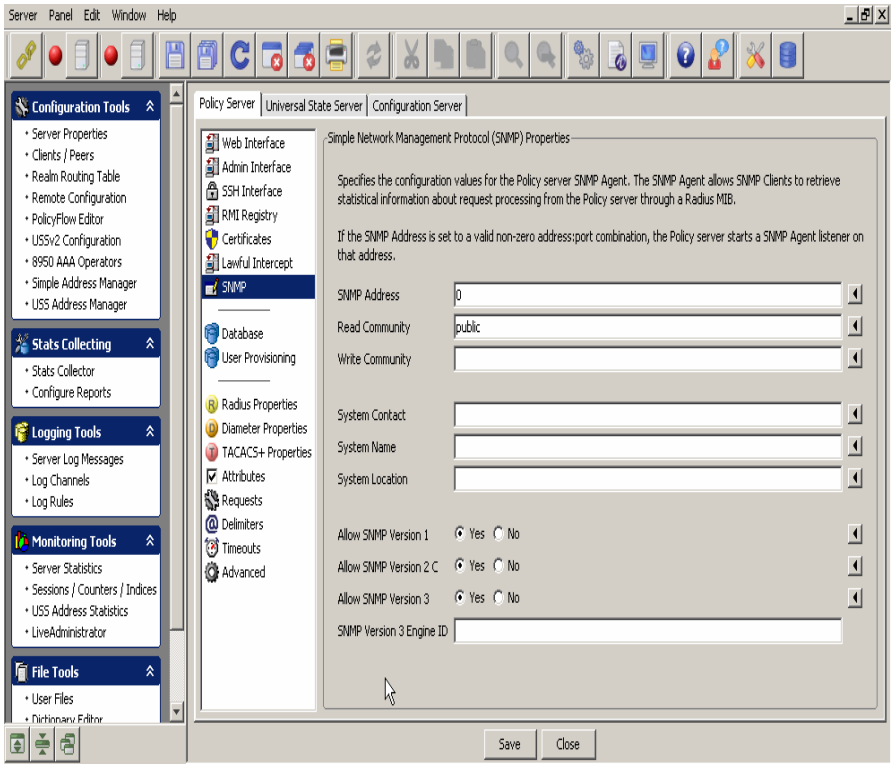
Configurable Properties	Description
Lawful Intercept Address	Specifies the address for lawful intercept target administrative messages. The value of zero (0) disables the address.

SNMP Panel

The SNMP properties can configure the SNMP agent built into the 8950 AAA server. 8950 AAA acts as an SNMP agent counting events that it receives.

To go to the Simple Network Management Protocol (SNMP) Properties panel, click on the **SNMP** option from the Policy Server data pane menu options on the left side. The SNMP properties panel is displayed as shown in Figure 4-7.

Figure 4-7 Policy Server-SNMP Properties Panel



The SNMP properties panel specifies the configuration values for the Policy server SNMP agent. The SNMP agent allows the SNMP clients to retrieve statistical information about request processing from the policy server through a Radius MIB.

If the SNMP address is set to a valid non-zero address:port combination, the policy server starts a SNMP agent listener on that address.

Table 4-7 lists the configurable entities of this panel.

Table 4-7 SNMP properties panel-Properties

Configurable Properties	Description
SNMP Address	Specifies the port to listen to the SNMP requests on. Entering a value of ‘0’ disables the listener. The SNMP address defaults to zero (0).
Read Community	Specifies the read community value that controls access to read variables. The read community value defaults to ‘public’.

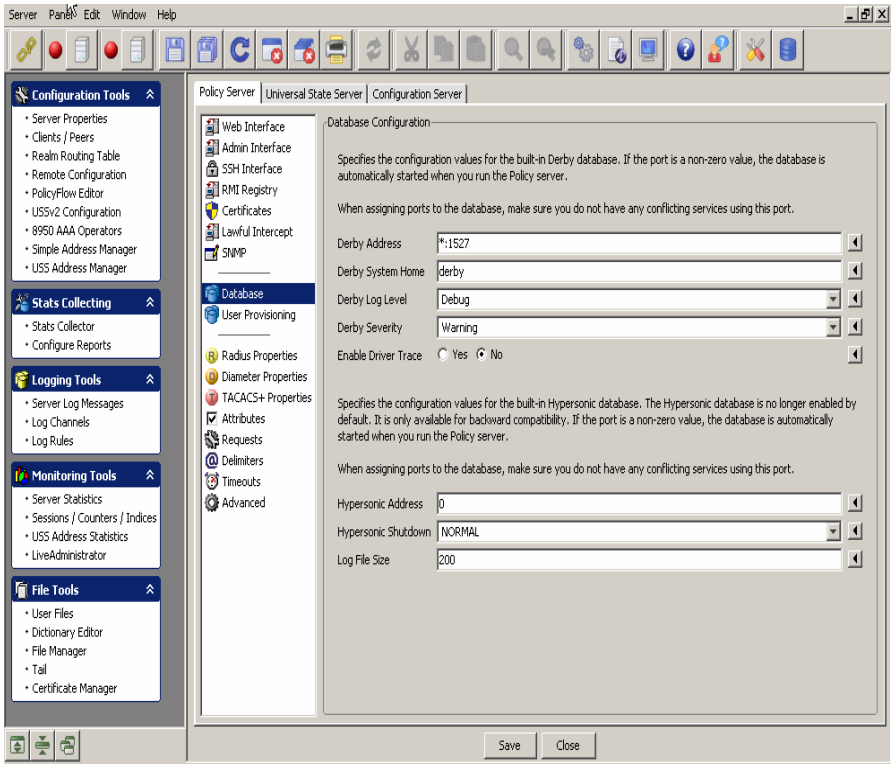
Table 4-7 SNMP properties panel-Properties

Configurable Properties	Description
Write Community	Specifies the write community value that controls access to write variables. The write community has no default values.
System Contact	Specifies the contact name of the SNMP agent.
System Name	Specifies the name of the SNMP agent.
System Location	Specifies the location of the SNMP agent.
Allow SNMP Version 1	If enabled, the policy server SNMP agent accepts version 1.
Allow SNMP Version 2 C	If enabled, the policy server SNMP agent accepts version 2 C.
Allow SNMP Version 3	If enabled, the policy server SNMP agent accepts version 3.
SNMP Version 3 Engine ID	This value must be globally unique and is calculated by the policy server upon start up using the proposed algorithm in RFC-3411 as follows: The first four octets of the engineID are set to the 8950 AAA enterprise number ‘831’ with the very first bit set to 1 (8000033f), octet number 5 is set to 01 to indicate an IPv4 address and finally octets 6 through 9 are set the servers IP address. This address is either the value of the server property SNMP address, or if that address is wildcard (*), the first non-loopback IPv4 address of the system. Setting the SNMP V3 engine ID value explicitly will disable the above algorithm and it is not recommended unless absolutely necessary.

Database Configuration Panel

To go to the Database Configuration panel, click on the **Database** option from the Policy Server data pane menu options on the left side. The Database Configuration panel is displayed as shown in Figure 4-8.

Figure 4-8 Policy Server-Database Configuration Panel



The Database Configuration panel specifies the configuration values for the built-in Derby database. If the port is a non-zero, the database is automatically started when you run the policy server.

> **Important!** When assigning ports to the database, make sure you do not have any conflicting services using this port.

This panel also specifies the configuration values for the built-in Hypersonic database. The Hypersonic database is no longer enabled by default. It is only available for backward compatibility. If the port is a non-zero value, the database is automatically started when you run the policy server.

> **Important!** When assigning ports to the database, make sure you do not have any conflicting services using the port.

Table 4-8 lists the configurable entities of this panel.

Table 4-8 Database Configuration Panel-Properties

Configurable Properties	Description
Derby Address	Sets the listen addresses for Apache Derby database server.

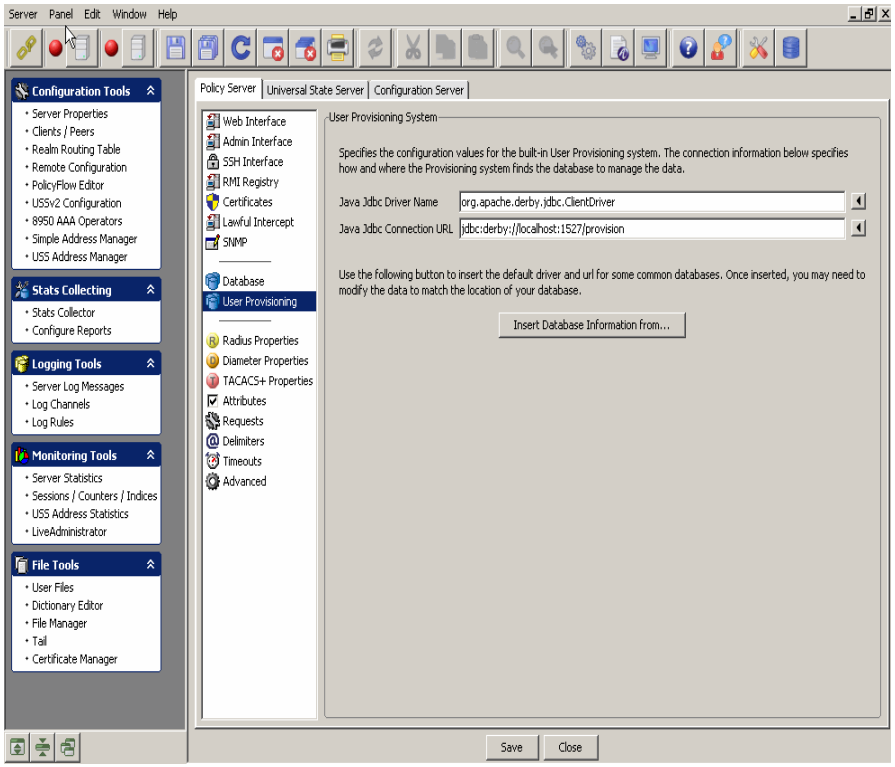
Table 4-8 Database Configuration Panel-Properties

Configurable Properties	Description
Derby System Home	Sets the location of the derby database files. This is the name of sub-directory under the 8950 AAA base installation directory. Sets the derby.system.home Derby property.
Derby Log level	Sets the 8950 AAA log level that messages from the Derby database server will be logged.
Derby Severity	Sets the level of the Derby messages that Derby will output to our logging system. These messages are logged at the Derby log level in the AAA logging system.
Enable Driver Trace	If enabled, the Derby driver level messages are logged in the policy server log.
Hypersonic configuration entity details	
Hypersonic Address	Sets the listen addresses for the Hypersonic database server.
Hypersonic Shutdown	Sets the shutdown mode for the database. NORMAL: Checkpoints the database normally. IMMEDIATELY: Equivalent to a poweroff or crash. COMPACT: Compacts the tables, closes the log, and checkpoints the database.
Log File Size	Sets the maximum size (in megabytes) that the database log file can reach before an automatic checkpoint occurs.

User Provisioning Panel

To go to the User Provisioning System panel, click on the **User Provisioning** option from the Policy Server data pane menu options on the left side. The User Provisioning System panel is displayed as shown in Figure 4-9.

Figure 4-9 Policy Server-User Provisioning System Panel



The User Provisioning system specifies the configuration values for the built-in User Provisioning system. The connection information below specifies how and where the provisioning system finds the database to manage the data.

Table 4-9 lists the configurable entities of this panel.

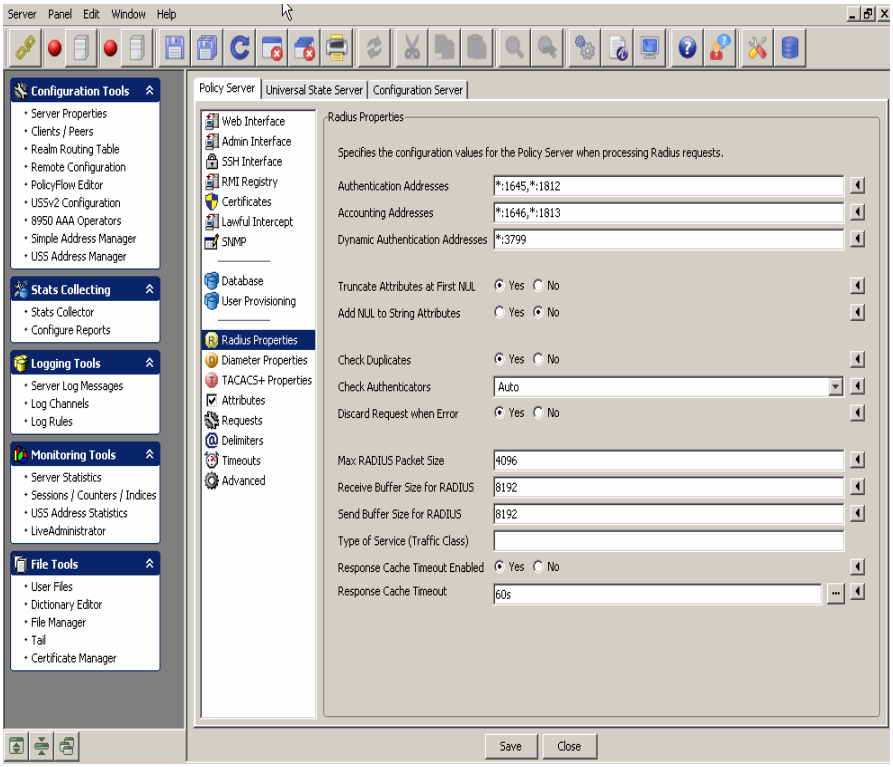
Table 4-9 User Provisioning System panel-Properties

Configurable Properties	Description
Java JDBC Driver name	The Java Jdbc driver name.
Java JDBC Connection URL	The Java Jdbc connection URL.
Insert Database Information from..	Click this to get a list of Database names that are available from which you can select any of the database type to insert the database information from.

Radius Properties Panel

To go to the RADIUS Properties panel, click on the **Radius Properties** option from the Policy Server data pane menu options on the left side. The Radius properties panel is displayed as shown in Figure 4-10.

Figure 4-10 Policy Server-RADIUS Properties Panel



The RADIUS properties panel specifies the configuration values for the Policy server when processing Radius requests.

Table 4-10 lists the configurable entities of this panel.

Table 4-10 Radius Properties panel-Properties

Configurable Properties	Description
Authentication Addresses	Sets the listening addresses for authentication requests. This value is a comma separated list of address:port values. If address is omitted, it is assumed to be *. If the port is omitted, it defaults to 1812. Default value is *:1645, *:1812. If this property is not defined or set to zero (0) authentication requests will not be processed.
Accounting Addresses	Sets the listening addresses for accounting requests. This value is a comma separated list of address:port values. If address is omitted, it is assumed to be *. If the port is omitted, it defaults to 1813. Default value is *:1646, *:1813. If this property is not defined or set to zero (0) authentication requests will not be processed.

Table 4-10 Radius Properties panel-Properties

Configurable Properties	Description
Dynamic Authentication Addresses	Sets the listening address for dynamic authentication requests. This value is a comma separated list of address:port values. If address is omitted, it is assumed to be *. If the port is omitted, it defaults to 3799.
Truncate Attributes at First NUL	If enabled, attributes are truncated at the first NUL found in the value. If disabled, the attribute values are not truncated. This enables support for NAS devices that send NUL characters in their attributes.
Add NUL to string attributes	If enabled, a NUL is appended to the end of plain string attributes in response requests to the NAS. This enables support for NAS devices that send NUL characters in their attributes.
Check Duplicates	If enabled, the server checks to see if the request received is a duplicate of a previously received request. Duplicates are detected by a combination of the Source IP, Source Port, and Packet Authenticator. The default setting is true. This property can be set on a per-client basis in the Client properties.
Check Authenticators	If enabled, the policy server checks the request authenticator and if not verified, the request is dropped.
Discard request when error	If enabled, the policy server discards packets when a method returns an error. If not enabled, the policy server rejects the packet.
Max RADIUS packet size	Specifies the maximum RADIUS packet size that is allowed. The default is 4096 bytes.
Receive buffer size for RADIUS	Specifies the size of the system UDP receive buffer assigned to the local socket.
Send buffer size for RADIUS	Specifies the size of the system UDP send buffer assigned to the local socket.
Type of Service (Traffic Class)	Specifies the traffic class or type-of-service octet in the RADIUS IP header.
Response Cache Timeout Enabled	If enabled, the policy server caches responses for the time specified in the corresponding timeout property. If not enabled, responses are not cached.

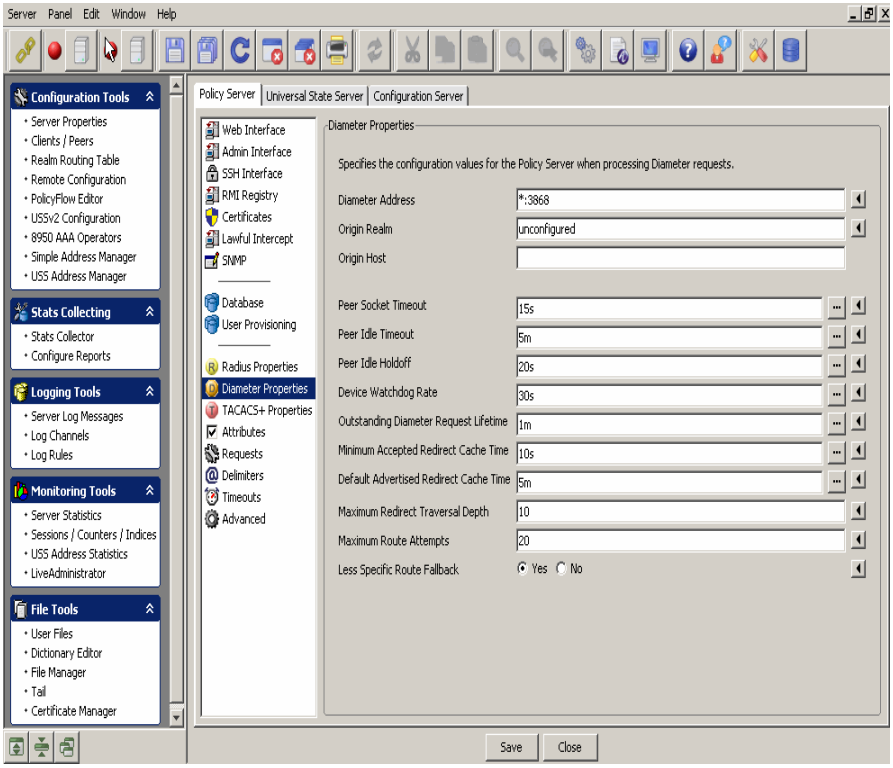
Table 4-10 Radius Properties panel-Properties

Configurable Properties	Description
Response Cache Timeout	When responding to the RADIUS requests, the policy server can remember (cache) the responses. If the response is sent, but lost and the NAS resends the same request, the policy server can respond with the cached response and not have to process the request again. This property sets how long the policy server keeps cached entries before discarding them.

Diameter Properties Panel

To go to the Diameter Properties panel, click on the **Diameter Properties** option from the Policy Server data pane menu options on the left side. The Diameter properties panel is displayed as shown in Figure 4-11.

Figure 4-11 Policy Server-Diameter Properties Panel



The Diameter properties panel specifies the configuration values for the Policy server when processing Diameter requests.

Table 4-11 lists the configurable entities of this panel.

Table 4-11 Diameter Properties panel-Properties

Configurable Properties	Description
Diameter Address	Sets the listen addresses for diameter requests. This value is a comma separated list of address:port values. If address is omitted, it is assumed to be *. If the port is omitted, it defaults to 3868. Default value is *:3868. If this property is not defined or set to zero (0) diameter requests will not be processed.
Origin Realm	Specifies the origin realm.
Origin Host	Specifies the origin host. Useful when testing diameter when no outside network connection is available.
Peer Socket Timeout	Specifies the amount of time (in milliseconds) allowed before generating a peer state machine 'Timeout' event as defined in RFC-3588, paragraph 5.6, during connection establishment with a remote peer. As an example, when an initiating peer attempts to connect to a remote peer in the Closed state, it starts a timer simultaneously with the connection request being sent. Then, in 'Wait-Conn-Ack', the state that follows Closed, a Timeout event is generated if no other event intervenes and the connection state is brought back to Closed while noting the peer as unavailable.
Peer Idle Timeout	Specifies the time in milliseconds the peer is timed out if idle.
Peer Idle Holdoff	Specifies the time in milliseconds before a peer is failed back after being suspended (if it was failed over at the time of suspension). Peers are getting suspended as a result of an idle-timeout, either on the local side or by the remote server requesting a connection shut down. Without this time-out and no extended requests, suspended peers would be kept in the failed over state indefinitely if they were failed over when asked to suspend.

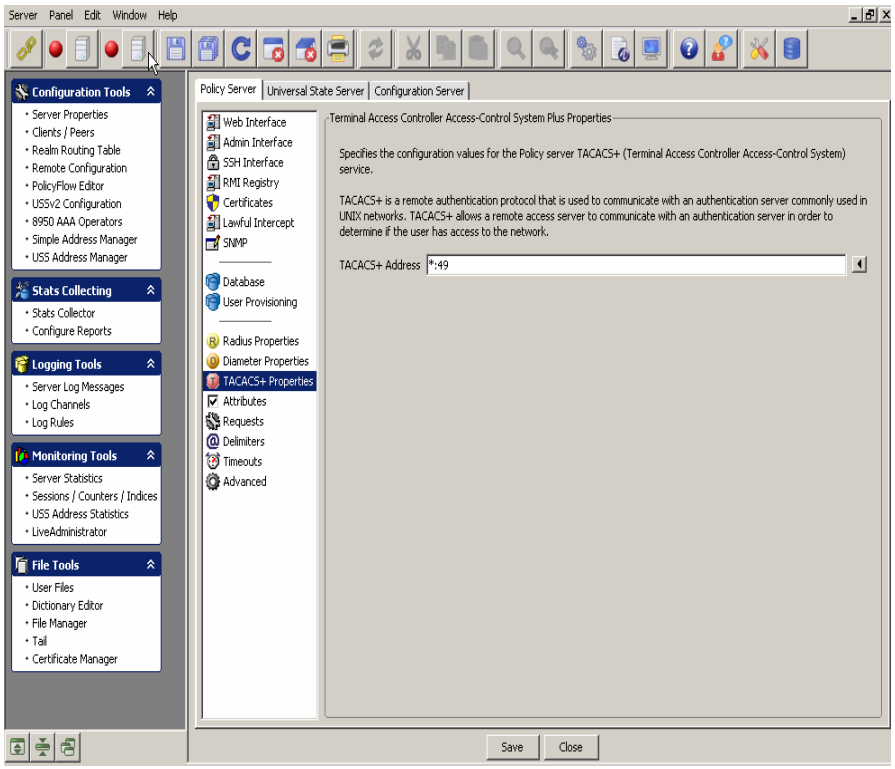
Table 4-11 Diameter Properties panel-Properties

Configurable Properties	Description
Device Watchdog Rate	The AAA Transport Profile document defines a heartbeat mechanism for maintaining connection state through the periodic exchange of 'Device-Watchdog' messages between two peers in their connected state. This parameter defines the average time (in milliseconds) between transmissions of consecutive 'Device-Watchdog-Request' message. Note that the time is an average for the local server as a random skew is applied to the value for each emitted watchdog request. The timer is also reset by other inter-peer traffic.
Outstanding Diameter Request Lifetime	Specifies how many milliseconds to keep an outbound request pending without an answer before it is discarded and a time-out event is sent back to the policy engine.
Minimum Accepted Redirect Cache Time	Specifies the minimum value accepted as a real value in a 'Redirect-Max-Cache-Time' AVP in a Diameter answer where result-code is set to DIAMETER-REDIRECT-INDICATION. If 'Redirect-Max-Cache-Time' is less than this value, the redirect indication is treated the same as a DONT-CACHE Redirect-Host-Usage indication.
Default Advertised Redirect Cache Time	Specifies the default value in seconds inserted into a locally generated redirect answer's 'Redirect-Max-Cache-Time' AVP if an explicit value is not defined by the policy flow.
Maximum Redirect Traversal Depth	The diameter server builds up a graph that models the received redirect indications as they are received (example, if the host alpha indicated redirection to beta and beta indicated redirection to gamma, the graph would be alpha -> beta -> gamma.) This parameter defines the maximum allowed depth of the redirection graph before a message is considered undeliverable.
Maximum Route Attempts	Specifies the maximum number of unique peers that are tried for routing of a request before returning an answer with DIAMETER_UNABLE_TO_DELIVER to the originator.
Less Specific Route Fallback	Setting to true enables fall-back to less specific route matching in the route table should all destinations in the current entry fail to accept the request.

TACACS+ Properties Panel

To go to the TACACS+ Properties panel, click on the **TACACS+ Properties** option from the Policy Server data pane menu options on the left side. The Terminal Access Controller Access-Control System Plus Properties panel is displayed as shown in Figure 4-12.

Figure 4-12 Policy Server-Terminal Access Controller Access-Control System Plus Properties Panel



The Terminal Access Controller Access-Control System Plus (TACACS+) Properties panel specifies the configuration values for the policy server TACACS+ service.

TACACS+ is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. TACACS+ allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

Table 4-12 lists the configurable entities of this panel.

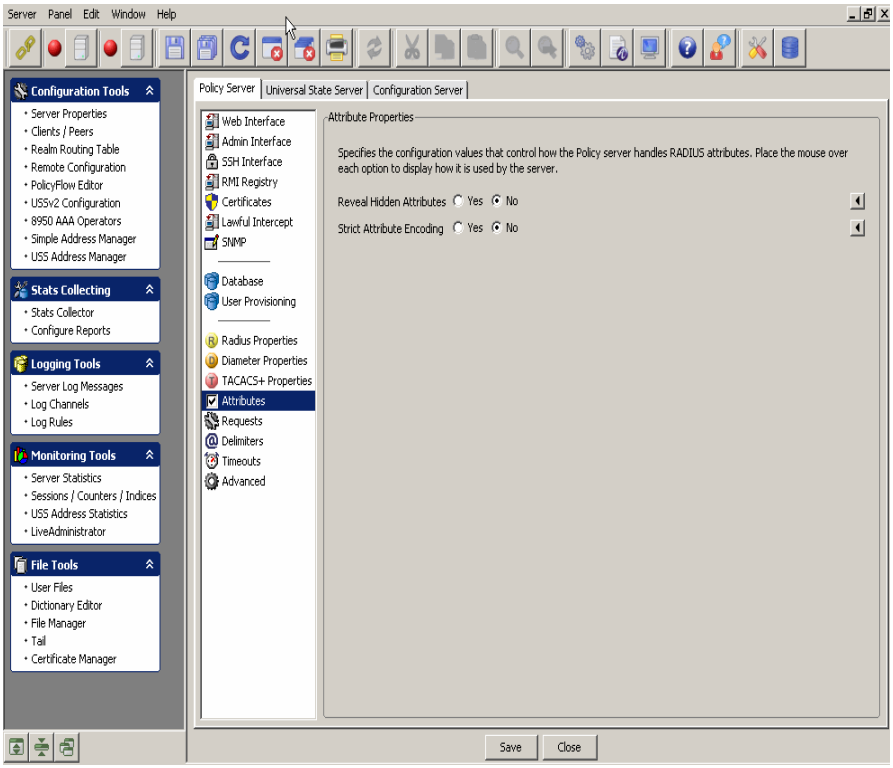
Table 4-12 TACACS+ Properties panel-Properties

Configurable Properties	Description
TACACS+ Address	Specifies the listener address that the policy server uses for the TACACS+ service.

Attribute Properties Panel

To go to the Attribute Properties panel, click on the **Attributes** option from the Policy Server data pane menu options on the left side. The Attribute Properties panel is displayed as shown in Figure 4-13.

Figure 4-13 Policy Server-Attribute Properties Panel



The Attribute Properties panel specifies the configuration values that control how the policy server handles RADIUS attributes. Place the mouse over each option to display how it is used by the server.

Table 4-13 lists the configurable entities of this panel.

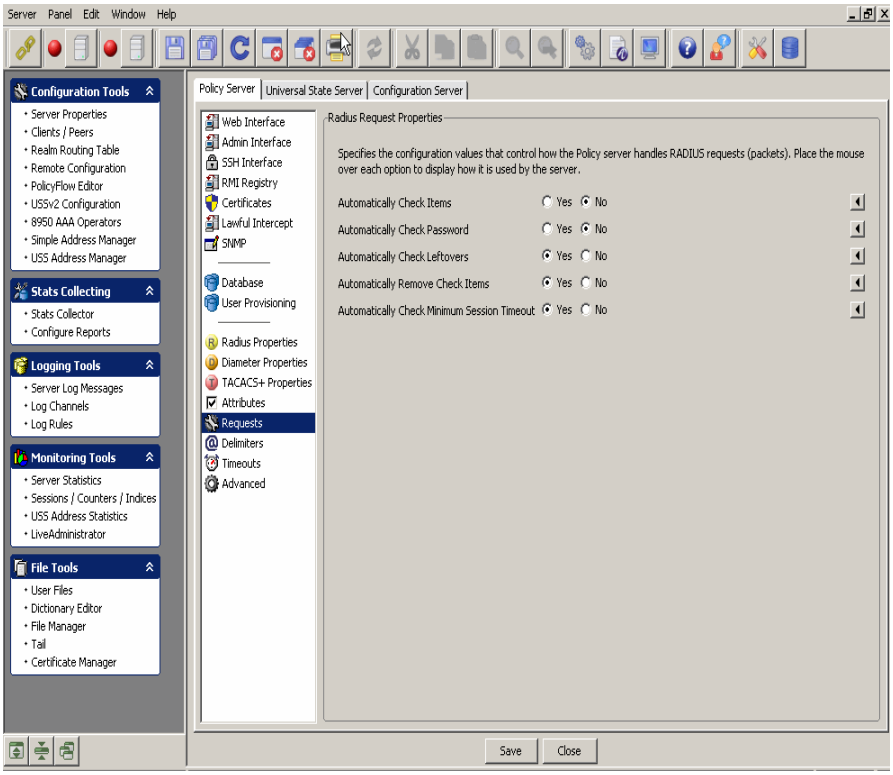
Table 4-13 Attribute Properties panel-Properties

Configurable Properties	Description
Reveal Hidden Attributes	Yes or No option. If enabled, attributes that are marked as hidden in the dictionary are now displayed in the packet trace.
Strict Attribute Encoding	Yes or No option. If enabled, attributes that can't be encoded cause an exception. If not enabled attributes that can't be encoded are skipped and not sent.

Requests Properties Panel

To go to the Requests Properties panel, click on the **Requests** option from the Policy Server data pane menu options on the left side. The Radius Request Properties panel is displayed as shown in Figure 4-14.

Figure 4-14 Policy Server-Radius Request Properties Panel



The Radius Request Properties panel specifies the configuration values that control how the policy server handles RADIUS requests (packets). Place the mouse over each option to display how it is used by the server.

Table 4-14 lists the configurable entities of this panel.

Table 4-14 Radius Request Properties panel-Properties

Configurable Properties	Description
Automatically Check Items	Yes or No option. If enabled, the policy server runs a check item plug-in equivalent at the end of the method chain.
Automatically Check Password	Yes or No option. If enabled, the policy server checks the password to the end of the method chain. This is similar to the AuthLocal plug-in.

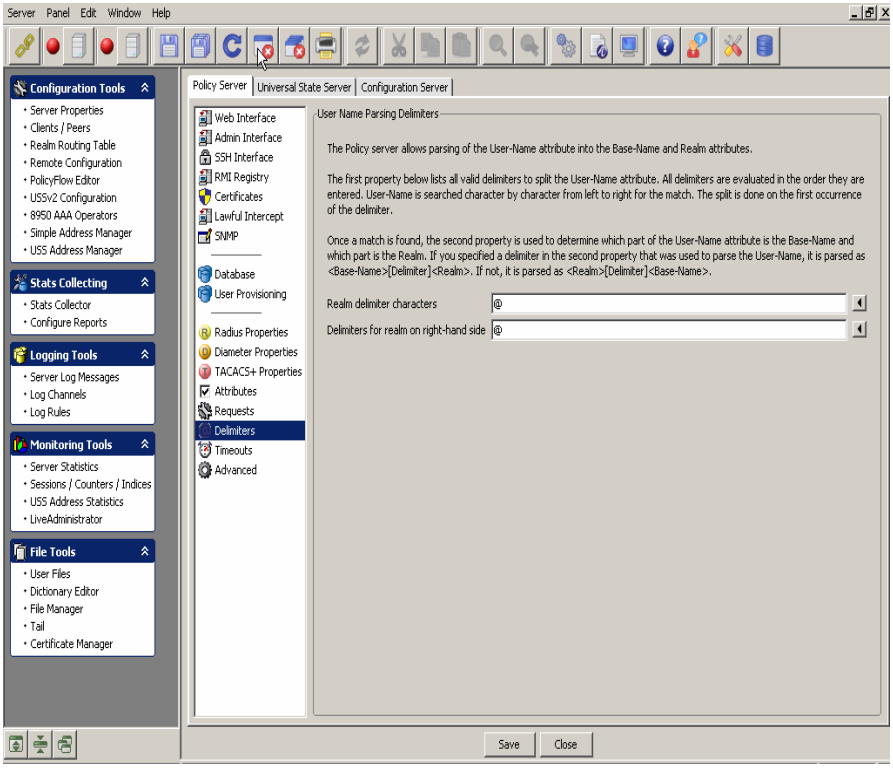
Table 4-14 Radius Request Properties panel-Properties

Configurable Properties	Description
Automatically Check Leftovers	Yes or No option. If enabled, the policy server rejects a request if there are check items left to be checked.
Automatically Remove Check Items	Yes or No option. If enabled, the policy server removes check items as they are checked by plug-ins.
Automatically Check Minimum Session Timeout	Yes or No option. If enabled, the policy server compares the minimum session timeout with the Time-of-Day value to decide whether to accept the request.

Delimiters Panel

To go to the User Name Parsing Delimiters panel, click on the **Delimiters** option from the Policy Server data pane menu options on the left side. The User Name Parsing Delimiters panel is displayed as shown in Figure 4-15.

Figure 4-15 Policy Server-User Name Parsing Delimiters Panel



The policy server allows parsing of the User-Name attribute into the Base-Name and Realm attributes.

The first property below lists all valid delimiters to split the User-Name attribute. All delimiters are evaluated in the order they are entered. User-Name is searched character by character from left to right for the match. The split is done on the first occurrence of the delimiter.

Once a match is found, the second property is used to determine which part of the User-Name attributes is the Base-Name and which part is the Realm. If you specified a delimiter in the second property that was used to parse the User-Name, it is parsed as <Base-Name>[Delimiter]<Realm>. If not, it is parsed as <Realm>[Delimiter]<Base-Name>.

Table 4-15 lists the configurable entities of this panel.

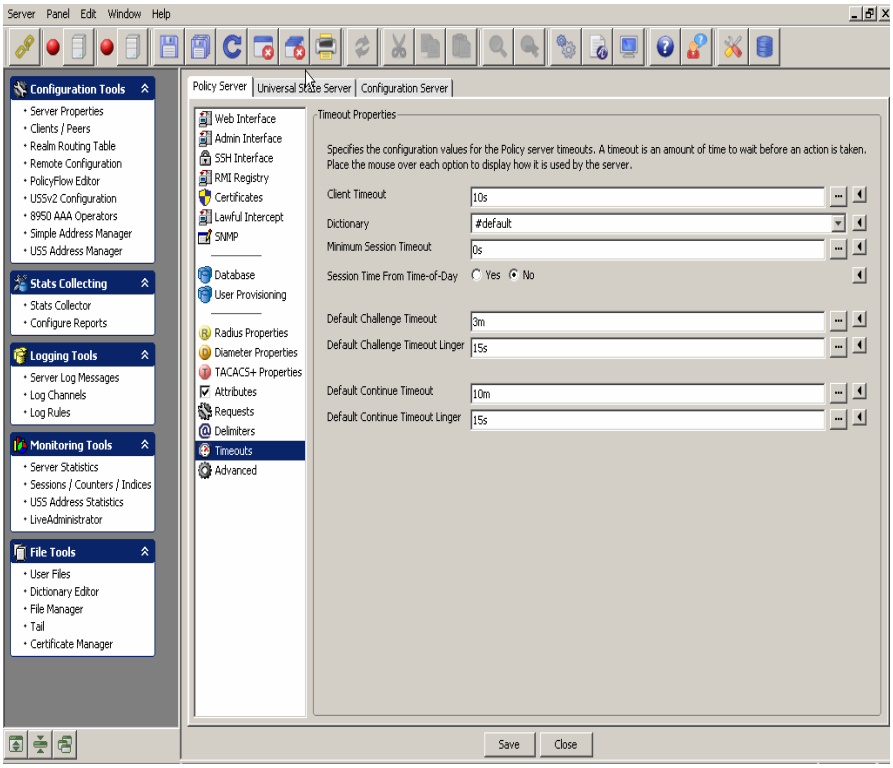
Table 4-15 User Name Parsing Delimiters Panel-Properties

Configurable Properties	Description
Realm delimiter characters	List of characters in search order to parse the user name into a user and realm. By default, the realm is the left hand value and the user is the right hand value, unless the delimiter is found in the 'Delimiters for realm on right side' value. The default when not specified is '@'.
Delimiters for realm on right-hand side	List of characters that mean the realm is the right hand value and the user is the left hand value of the parsed user name. This list should be a subset of the Realm Delimiter characters. The default when not specified is '@'.

Timeout Properties Panel

To go to the Timeout Properties panel, click on the **Timeouts** option from the Policy Server data pane menu options on the left side. The Timeout Properties panel is displayed as shown in Figure 4-16.

Figure 4-16 Policy Server-Timeout Properties Panel



The Timeout properties panel specifies the configuration values for the Policy server timeouts. A timeout is an amount of time to wait before an action is taken. Place the mouse over each option to display how it is used by the server.

Table 4-16 lists the configurable entities of this panel.

Table 4-16 Timeout Properties Panel-Properties

Configurable Properties	Description
Client Timeout	Time, in milliseconds, to specify the amount of time the policy server will wait before it discards the requests. This should match the timeout set on your NAS client.
Dictionary	Specifies the dictionary name to use for this client class definition.
Minimum Session Timeout	The policy server will reject any request that has a session-time value less than the value specified by the property. If reply.session-time is not set then no action is needed.
Session Time from Time-of-Day	If enabled, the session time is the time remaining from the Time-of-Day check item.

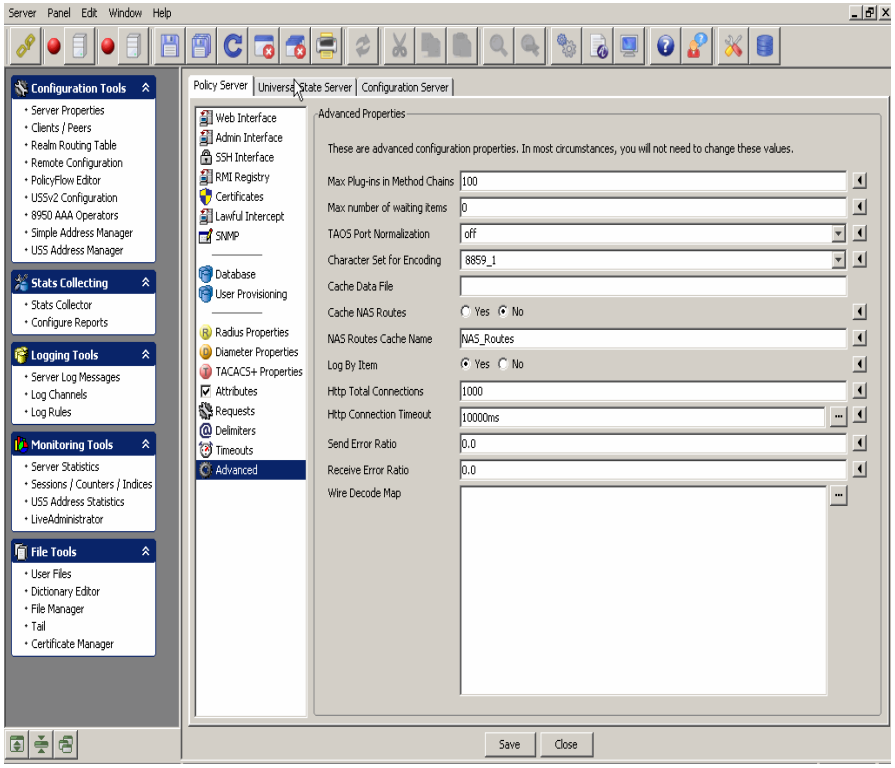
Table 4-16 Timeout Properties Panel-Properties

Configurable Properties	Description
Default Challenge Timeout	Default Challenge Timeout. Duration with default timeunit in seconds.
Default Challenge Timeout Linger	Default challenge timeout linger. Duration with default timeunit in seconds.
Default Continue Timeout	Default continue timeout. Duration with default timeunit in seconds.
Default Continue Timeout Linger	Default continue timeout linger. Duration with default timeunit in seconds.

Advanced Properties Panel

To go to the Advanced Properties panel, click on the **Advanced** option from the Policy Server data pane menu options on the left side. The Advanced Properties panel is displayed as shown in Figure 4-17.

Figure 4-17 Policy Server-Advanced Properties Panel



The Advanced properties panel reflects the advanced configuration properties. In most circumstances, you will not need to change these values.

Table 4-17 lists the configurable entities of this panel.

Table 4-17 Advanced Properties Panel-Properties

Configurable Properties	Description
Max Plug-ins in Method Chains	Specifies the maximum number of plug-in invocations for ISPs. The default is 100.
Max number of waiting items	Specifies the maximum number of RADIUS items that can be waiting to be processed by the policy server. The default is 0, which means no limit. **Important!** Setting this to small numbers (for example, less than 10) will greatly diminish server performance.
TAOS Port Normalization	Specifies how to get the real NAS port number out of the NAS port info. This should only be used if your NASs are running TAOS.
Character Set for Encoding	Specifies the character set to use to encode string attributes in requests.
Cache Data File	Specifies the file that contains the ‘cache’ data when using the ReadCache and WriteCache plugins. If specified, the contents of the ‘cache’ is written to this file on policy server shutdown and read into the cache on policy server startup.
Cache NAS Routes	Yes or No option. Specifies whether NAS IP address and Client IP address (proxy) are stored in the NAS Routes cache.
NAS Routes Cache Name	Specifies the name of the cache to store NAS Routes within the policy server.
Log By Item	Yes or No option. If enabled, the policy server groups all messages of a request together when the messages are logged. If not enabled, messages from different requests could overlap in the log output.
HTTP Total Connections	Sets the maximum number of concurrent HTTP connections to make as a client.
HTTP Connection Timeout	Sets the timeout in milliseconds used when retrieving an HTTP connection from the HTTP connection manager. 0 means to wait indefinitely.

Table 4-17 Advanced Properties Panel-Properties

Configurable Properties	Description
Send Error Ratio	Sets a simulated transmit error ratio for server. When set to a non-zero value, RADIUS packets transmitted from the work engine will be randomly dropped. If set to one, all packets will be dropped.
Receive Error Ratio	Sets a simulated receive error ratio for server RADIUS listeners. When set to a non-zero value, RADIUS listener threads will randomly drop received RADIUS packets. A value of one will drop all packets.
Wire Decode Map	Specifies how to read the request from the wire (decode) into the policy server. If not specified, '${request.*}:=${*};' is used. Use an '@' symbol to reference a file, example, @filename.

Universal State Server tab

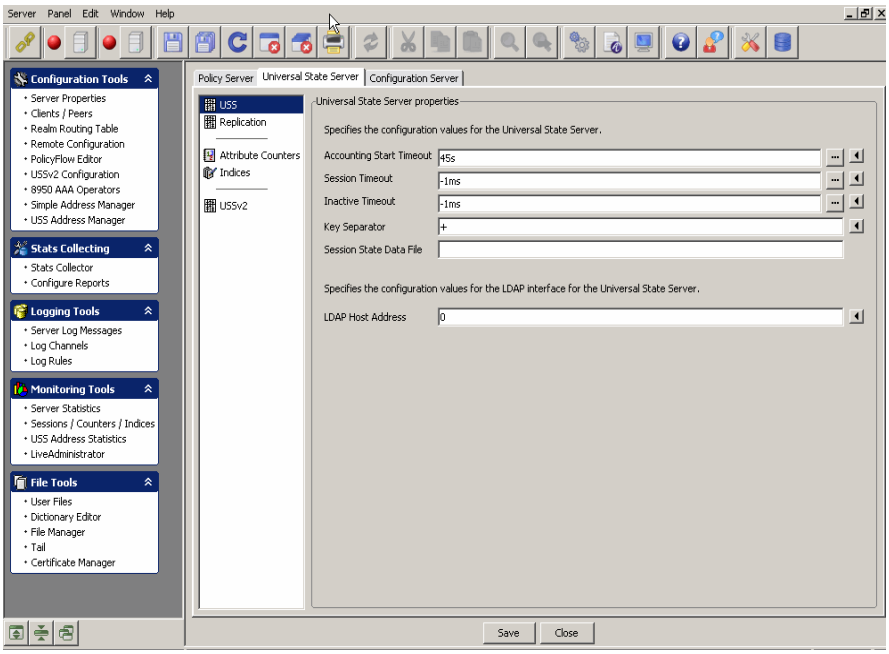
About the Universal State Server tab

The Universal State Server (USS) is an in-memory database optimized to track network-resource usage. It interacts with the 8950 AAA server to maintain usage counts and enforce resource limits within the network.

The Universal State Server tab allows you to configure the entities in the Universal State Server.

To go to the Universal State Server panel, click on the **Universal State Server** tab in the Server Properties navigation option. The Universal State Server properties tab is displayed as shown in Figure 4-18.

Figure 4-18 Universal State Server Properties Panel



USS Panel

When you click on the **Universal State Server** tab option, by default, the Universal State Server properties panel is displayed as shown in Figure 4-18.

The Universal State Server properties panel specifies the configuration values for the Universal State Server.

Table 4-18 lists the configurable entities of this panel.

Table 4-18 Universal State Server Panel-Properties

Configurable Properties	Description
Accounting Start Timeout	Specifies the time (in milliseconds) the Universal State Server will wait for an accounting-start after recording an access-accept for a particular port.
Session Timeout	Specifies the time (in milliseconds) after which the Universal State Server will mark a port as idle.
Inactive Timeout	Specifies the time (in milliseconds) after which an inactive session entry will be removed entirely. A value of -1 disables the timeout and 0 fires immediately. The default value is -1 (disabled).

Table 4-18 Universal State Server Panel-Properties

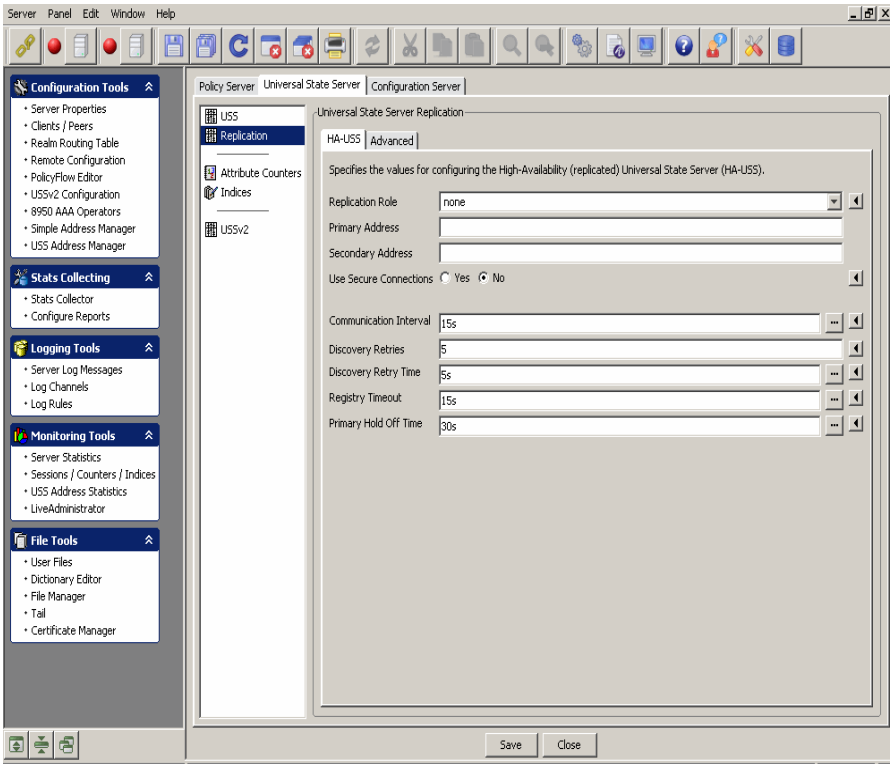
Configurable Properties	Description
Key Separator	Specifies the character that separates the key into two parts for the creation of secondary indices. This character should not appear in the values used to construct the key (that is, the NAS-IP-Address and NAS-Port).
Session State Data File	Specifies a file to store the session state information. If specified, the state server saves the session information when it shuts down. When the state server is restarted the initial session information is read from this file. **Important!** This file is deleted after read and created each time the state server shuts down.
LDAP interface information–Specifies the configuration values for the LDAP interface for the Universal State Server	
LDAP Host Address	Specifies the listener address that the policy server uses for the LDAP interface to the stateserver.

Replication Panel

To go to the Universal State Server Replication panel, click on the **Replication** option from the Universal State Server data pane menu options on the left side.

The Universal State Server Replication panel has two tabs, the **HA-USS** tab and the **Advanced** tab. By default, the HA-USS tab panel is displayed as shown in Figure 4-19.

Figure 4-19 Universal State Server Replication Panel with HA-USS tab



The HA-USS tab in the Universal State Server Replication panel specifies the values for configuring the high-availability (replicated) universal state server (HA-USS).

Table 4-19 lists the configurable entities of this panel.

Table 4-19 Universal State Server Replication Panel-HA-USS tab properties

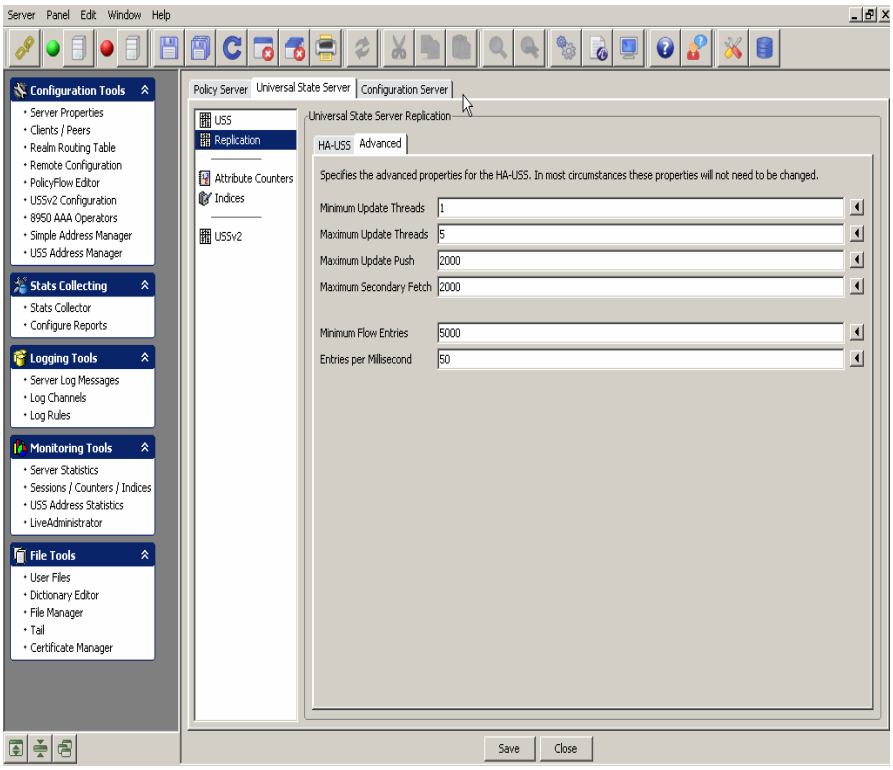
Configurable Properties	Description
Replication Role	Specifies the role of the stateserver on this server.
Primary Address	Specifies the host and address of the state server (the embedded registry). On the secondary, this should be set to the primary host name, and on the primary can be either “localhost” or the primary host name. If a non-default port is desired, specify it as localhost:9089.
Secondary Address	Specifies the host and address of the state server (the embedded registry) to use in an replicated USS Address Manager configuration. On the primary, this should be set to the secondary host name. If a non-default port is desired, specify it as localhost:9089.

Table 4-19 Universal State Server Replication Panel-HA-USS tab properties

Configurable Properties	Description
Use Secure Connections	Yes or No option. Specifies to use secure connections (SSL) for registry connections and communications between the primary and secondary state servers.
Communication Interval	Specifies how often (in milliseconds) that the state server communicates with the primary state server.
Discovery Retries	Specifies the number of times to attempt to find the primary state server.
Discovery Retry Time	Specifies the time (in milliseconds) to wait between each failed attempt to find the primary state server.
Registry Timeout	Specifies the maximum amount of time (in milliseconds) to allow before a remote registry access aborts the attempt.
Primary Hold Off time	Specifies the amount of time (in milliseconds) that the primary will wait to receive updates from the secondary. This only occurs when the primary shuts down and is restarted.

On the Universal State Server Replication panel, click on the **Advanced** tab. The Advanced tab panel is displayed as shown in Figure 4-20.

Figure 4-20 Universal State Server Replication Panel with Advanced tab



The Advanced tab in the Universal State Server Replication panel specifies the advanced properties of the HA-USS. In most circumstances these properties will not need to be changed.

Table 4-20 lists the configurable entities of this panel.

Table 4-20 Universal State Server Replication panel-Advanced tab properties

Configurable Properties	Description
Minimum Update Threads	Specifies the minimum number of worker threads per replication update queue.
Maximum Update Threads	Specifies the maximum number of worker threads per replication update queue.
Maximum Update Push	Specifies the maximum number of USS entries to push to a secondary in a single RMI call.
Maximum Secondary Fetch	Specifies the maximum number of USS entries for the primary to fetch from the secondary in a single RMI call during reconciliation.

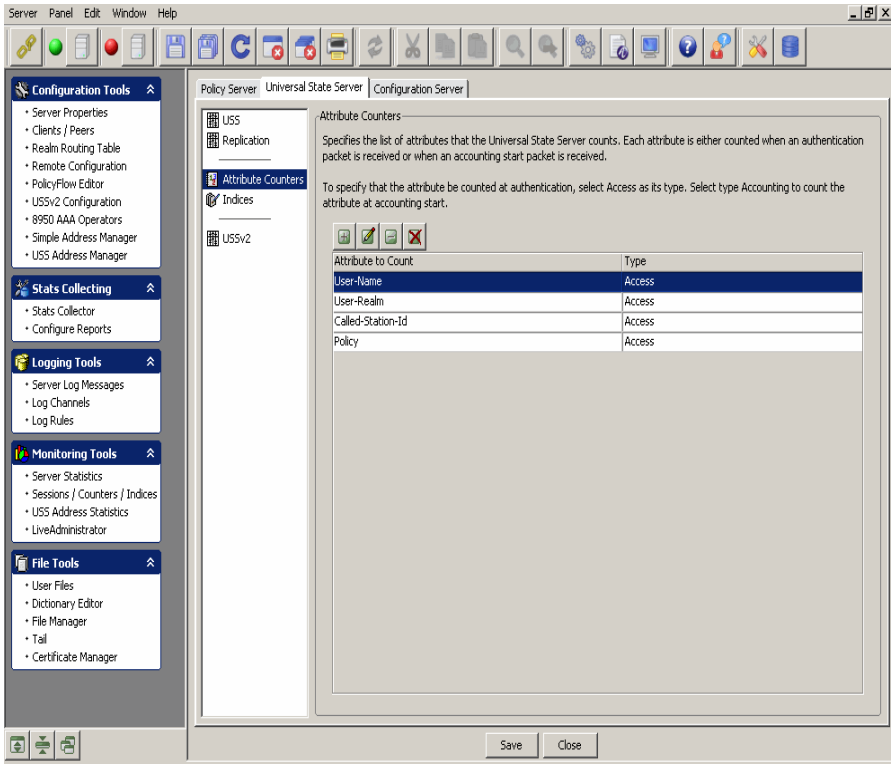
Table 4-20 Universal State Server Replication panel-Advanced tab properties

Configurable Properties	Description
Minimum Flow Entries	Sets the minimum number of entries in the primary replication queue before plug-in flow control enables.
Entries per Millisecond	Used to compute the flow control delay time for the stateserver plug-in.

Attribute Counters Panel

To go to the Attribute Counters panel, click on the **Attribute Counters** option from the Universal State Server panel menu options on the left side. The Attribute Counters panel is displayed as shown in Figure 4-21.

Figure 4-21 Universal State Server-Attribute Counters



The Attribute Counters panel specifies the list of attributes that the Universal State Server counts. Each attribute is either counted when an authentication packet is received or when an accounting start packet is received.

To specify that the attribute be counted at authentication, select Access as its type. Select the type Accounting to count the attribute at accounting start.

A table is displayed that lists the attributes to count and specifies the type of the attribute. Four action buttons are also displayed above the table that allows you to perform the actions specified in Table 4-21.

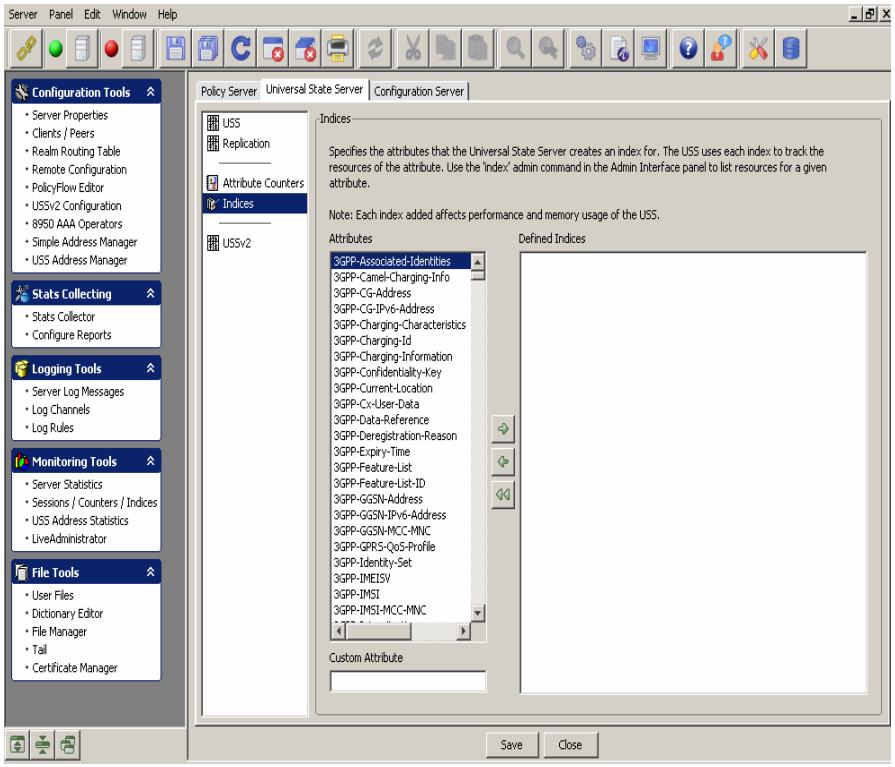
Table 4-21 Universal State Server-Attribute Counters

Action Buttons	Description
	Inserts a record.
	Edits the selected record.
	Deletes the selected record.
	Deletes all the records.

Indices Panel

To go to the Indices panel, click on the **Indices** option from the Universal State Server panel menu options on the left side. The Indices panel is displayed as shown in Figure 4-22.

Figure 4-22 Universal State Server-Indices



The Indices panel specifies the attributes that the Universal State Server creates an index for. The USS uses each index to track the resources of the attribute. Use the ‘index’ admin command in the Admin Interface panel to list resources for a given attribute.

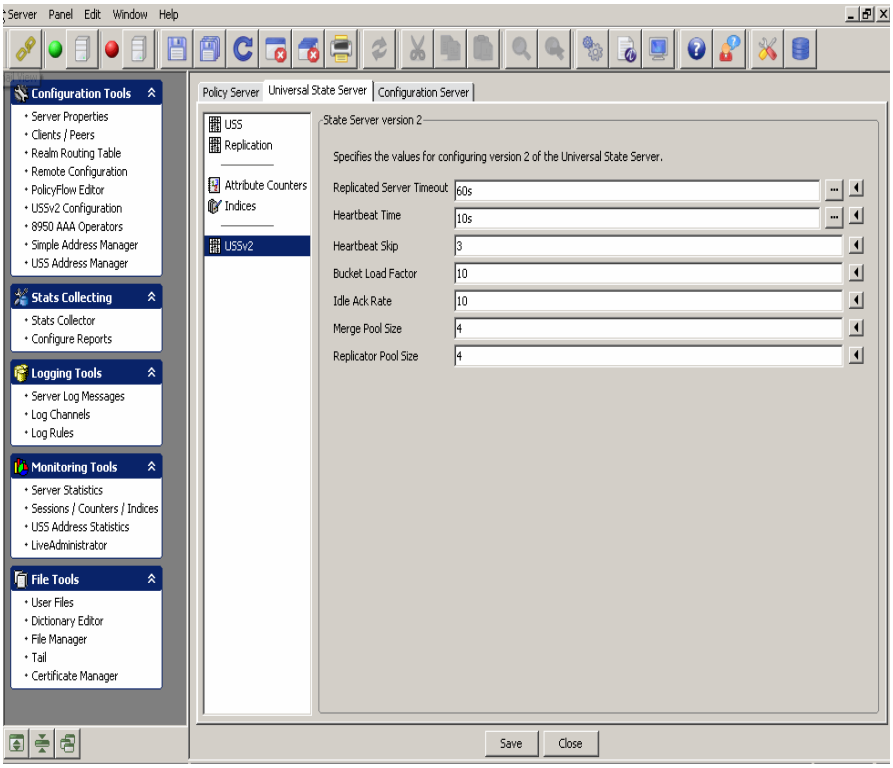
> **Important!** Each index added affects the performance and memory usage of the USS.

The Indices panel shows the existing Attributes in the Universal State Server in one side of the panel and allows you to select and add any of these attributes to the Defined Indices window using the action arrow buttons in between these windows. You can choose to add an item, delete selected record, or delete all records from the Defined Indices window.

USSv2 panel

To go to the State Server version 2 panel, click on the **USSv2** option from the Universal State Server data pane menu options on the left side. The State Server version 2 panel is displayed as shown in Figure 4-23.

Figure 4-23 State Server version 2 Panel



The State Server version 2 panel specifies the values for configuring the version 2 of the universal state server.

Table 4-22 lists the configurable entities of this panel.

Table 4-22 State Server version 2 panel properties

Configurable Properties	Description
Replicated Server Timeout	Specifies the amount of time the replication queue is kept active after a replicated server has gone down.
Heartbeat Time	Specifies the amount of time between heartbeat transmissions.
Heartbeat Skip	Specifies the number of missing heartbeats before a connection to a replicated server is considered down.
Bucket Load Factor	Specifies the maximum number of heartbeat intervals of outstanding buckets before replication is halted and a reconciliation is prepared.

Table 4-22 State Server version 2 panel properties

Configurable Properties	Description
Idle Ack Rate	When remote ack rate per heartbeat interval drops below this limit a prepared reconciliation is started.
Merge Pool Size	Specifies the number of threads servicing inbound replication.
Replicator Pool Size	Specifies the number of threads servicing outbound replication.

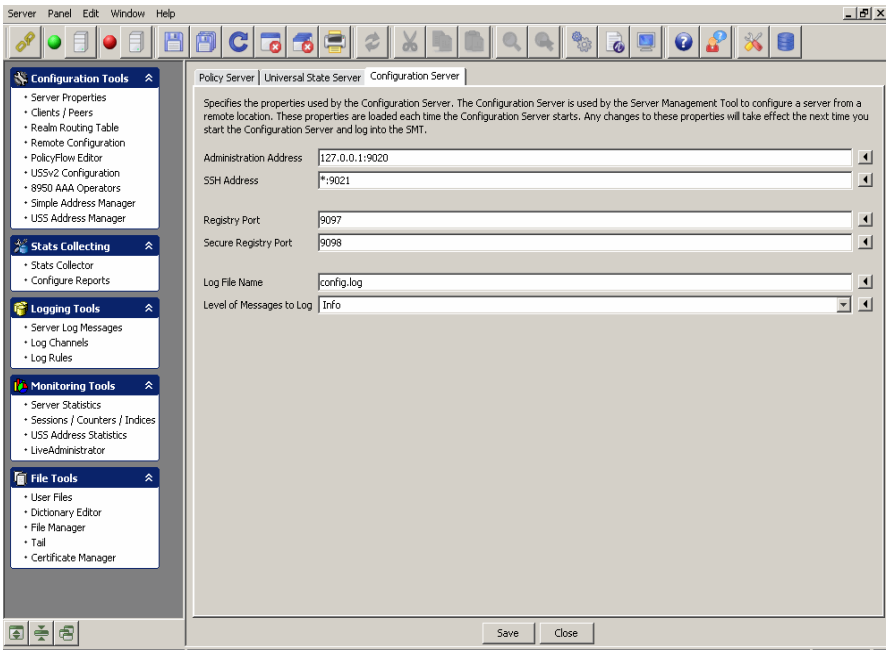
Configuration Server tab

About the Configuration Server tab

The Configuration Server tab allows you to configure the entities in the Configuration Server.

To go to the Configuration Server panel, click on the **Configuration Server** tab in the Server Properties navigation option. The Configuration Server panel is displayed as shown in Figure 4-24.

Figure 4-24 Configuration Server Panel



The Configuration Server panel specifies the properties used by the configuration server. The configuration server is used by the Server Management Tool to configure a server from a remote location. These properties are loaded each time the configuration server starts. Any changes to these properties will take effect the next time you start the configuration server and log into the SMT.

Table 4-23 lists the configurable entities of this panel.

Table 4-23 Configuration Server Panel properties

Configurable Properties	Description
Administration Address	Specifies the TCP/IP address on which the Admin interface listens for connections. The address is in the form of a hostname (or "*") followed by a colon, followed by the port number. The hostname must be a name that corresponds to a local interface on the machine, or the value "*", which represents all local interfaces. The default value for this property is "*.9020".
SSH Address	Specifies the address and port the server listens to, default is "*:9021" and a port number of 0 means do not start SSH at all.
Registry Port	Defines the port to be used when creating an RMI registry. Normally, an RMI registry is already running at the address specified. However, if there is no registry, the configuration server will try to create one on the local host. By default, it uses the RMI port 9097 to do this, but this property enables another port to be used if necessary.
Secure Registry Port	Secure registry port.
Log File Name	Specifies the name of the file in which configuration server writes messages and errors. The file 'config.log' is the default log file name.
Level of Messages to Log	Specifies the level (or debug level). The level determines what type of messages the configuration server to the log file. By default, the configuration server logs at 'info' level.

END OF STEPS

5 Configuring 8950 AAA Client Properties

Overview

Purpose

This chapter discusses the process of configuring clients (NASs or other access points) with the 8950 AAA Server Management Tool. Use the **Clients** panel to identify the clients with whom your 8950 AAA server communicates during request processing. Refer to your client product documentation for information specific to its configuration options.

The following topics are included in this chapter:

Introduction

Upon receiving a RADIUS request, 8950 AAA must first determine that the request is from an authorized RADIUS client. The source of the request is validated before the request is accepted for processing. The server uses the source IP address or domain name of the data packet to locate client information stored in a special 8950 AAA file called the *clients file*. The clients file is maintained using the Clients panel of the SMT. Messages from unknown clients are logged and then discarded.

Configuring Clients

About Configuring Clients

A RADIUS client (NAS or other resource with RADIUS client capabilities) passes session information to designated RADIUS servers and acts on the response returned. The 8950 AAA server must have the following information for each client that sends RADIUS requests to the server:

- IP address or domain name of the client
- A shared secret used between the server and the client

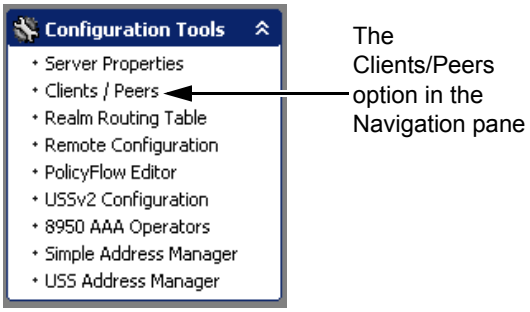
Important! Do not add entries for remote servers that will receive requests provided from the 8950 AAA server unless requests are also received directly from this remote server.

Using the SMT to Configure Clients

This section describes how to configure a 8950 AAA client. The specific procedure that follows lists steps to modify an existing client using the Server Management Tool. For information about running the SMT, please refer to "Starting the Server Management Tool".

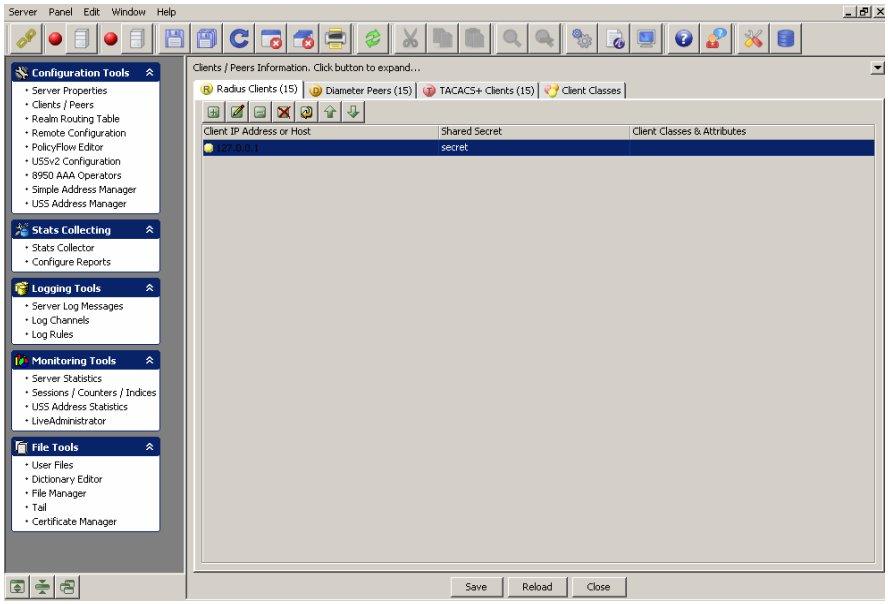
1. Select **Clients/Peers** from the Configuration Tools folder on the Navigation pane, as shown in Figure 5-1.

Figure 5-1 Navigation Pane-Clients/Peers option



Result: The 8950 AAA client/peer panel is displayed as shown in Figure 5-2.

Figure 5-2 The 8950 AAA SMT-Clients/Peers panel



The **Clients/Peers** panel (Figure 5-2) contains four tabs as following:

- Radius Clients
- Diameter Peers
- TACACS+ Clients
- Client Classes

When you click on the **Clients/Peers** in the navigation pane, by default, the *Radius Clients* tab is displayed as showed in Figure 5-2. Click on the other tabs like the *Diameter Peers* tab, the *TACACS+ Clients* tab, and the *Client Classes* tab to display information related to that screen. The following sections in this chapter explain each of these tabs in detail.

Using the Client/Peers SMT Action buttons

The **Client/Peers** menu bar also consists of a set of Action Buttons that appear at the top of the 8950 AAA client/peer panel, as shown in Figure 5-2.

The Action buttons are as shown in Figure 5-3.

Figure 5-3 Client/Peers-Action buttons

You can perform the following actions using these action buttons:

- Insert a record
- Edit selected record
- Delete selected record

- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

The Radius Clients tab

Radius Clients tab

The **Radius Clients** tab displays information about Radius Clients in different columns.

Table 5-1 displays the **Radius Clients** tab information.

Table 5-1 Client/Peers SMT-Radius Clients tab information

Column Name	Description
Client IP Address or Host	The client IP address, host name, or Fully Qualified Domain Name (FQDN).
Shared Secret	The secret key shared between the 8950 AAA server and the client. The shared secret must be entered exactly the same way on both the 8950 AAA and the client. Errors in entering the secret key is one of the most common causes of 8950 AAA configuration problems.
Client classes & Attributes	This section shows the names of any Client Classes to which this client has been assigned. In addition, any properties (specific Attribute Value Pairs (AVPs) assigned to the client are displayed. If it contains #default then there are no assigned classes or attributes for the client.

To go to the **Radius Client Properties** panel, click on the  action button. The **Radius Client Properties** panel is displayed as shown in Figure 5-4. This panel allows you to add or insert records to the Radius Client Properties. The **Radius Client Properties** panel, as shown in Figure 5-4, has the following three tabs:

- The **Radius Client Properties** tab that allows to add a record.
- The **Client Classes and Attributes** tab that allows to select the required client option.
- The **Comment** tab that allows to enter necessary comments.

Using the Radius Client Properties tab to Add a record

The **Radius Client Properties** tab allows you to add a record and enter information in the required fields as shown in Figure 5-4.

Figure 5-4 The Radius Client Properties-Add record panel

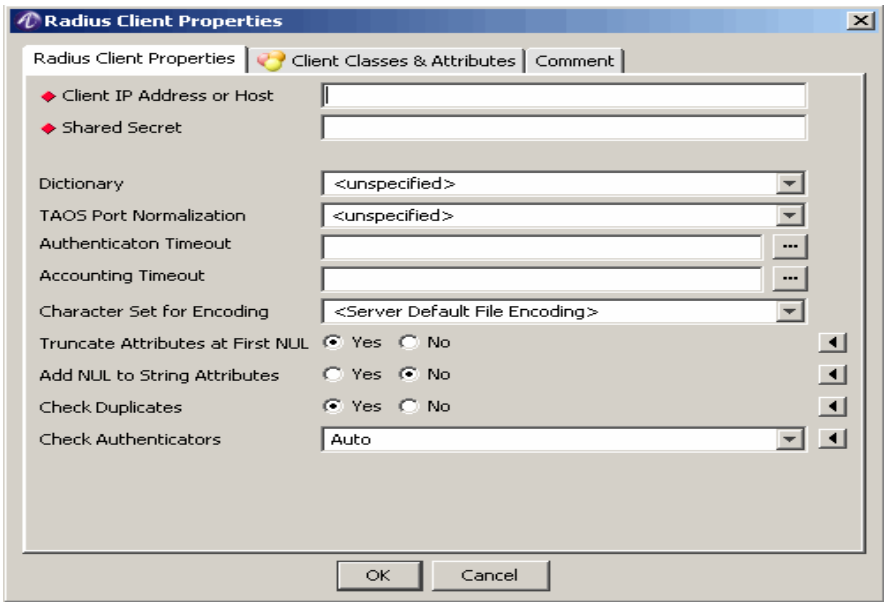


Table 5-2 explains each of these fields and the field descriptions.

Table 5-2 Radius Client Properties

Field Name	Description
Client IP Address or Host	Specifies the Domain name, IP Address, range of IP addresses, or a CIDR block of addresses.
Shared Secret	Shared secret between Policy server and client.
Dictionary	This section shows the names of any Client Classes to which this client has been assigned. In addition, any properties (specific Attribute Value Pairs (AVPs) assigned to the client are displayed. If it contains #default then there are no assigned classes or attributes for the client.
TAOS Port Normalization	Specifies how to get the real NAS port number out of the NAS port info. This should only be used if your NASs are running TAOS.

Table 5-2 Radius Client Properties

Field Name	Description
Authentication Timeout	Specifies the time, in milliseconds, the Policy server will wait before it discards authentication requests. This overrides the Client Timeout value for authentications only.
Accounting Timeout	Specifies the time, in milliseconds, the Policy server will wait before it discards accounting requests. This overrides the Client Timeout value for accounting requests only.
Character Set for Encoding	Specifies the character set to use to encode string attributes in requests.
Truncate Attributes at First NUL	Yes or No option. If enabled, attributes are truncated at the first NUL found in the value. If disabled, the attribute values are not truncated. This enables support for NAS devices that send NUL characters in their attributes.
Add NUL to String Attributes	Yes or No option. If enabled, a NUL is appended to the end of plain string attributes in response requests to the NAS. This enables support for NAS devices that send NUL characters in their attributes.
Check Duplicates	Yes or No option. If enabled, the server checks to see if the request received is a duplicate of a previously received request. Duplicates are detected by a combination of the Source IP, Source Port, and Packet Authenticator. The default setting is true. This property can be set on a pre-client basis in the Client Properties.
Check Authenticators	The drop-down list box displays the Auto, On, or OFF options. If enabled, the Policy server checks the request authenticator and if not verified, the request is dropped.

Using the Client Classes & Attributes tab in Radius Client Properties panel

The **Client Classes & Attributes** is one of the tabs in the **Radius Client Properties** Panel. This panel allows you to perform the following actions using the action buttons:

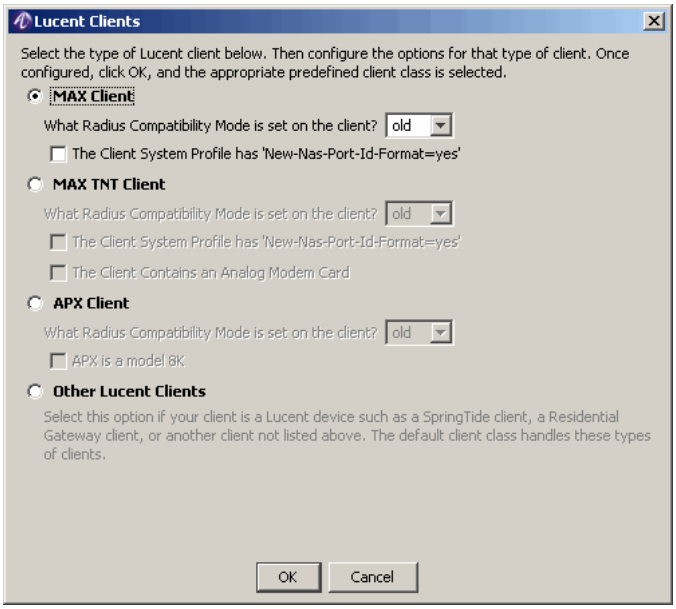
- Insert Row Wizard
- Insert a record
- Edit selected record

- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform the following actions using these action buttons:

1. The **Insert Row Wizard** action button displays the **Alcatel-Lucent Clients** dialog, as displayed in Figure 5-5.

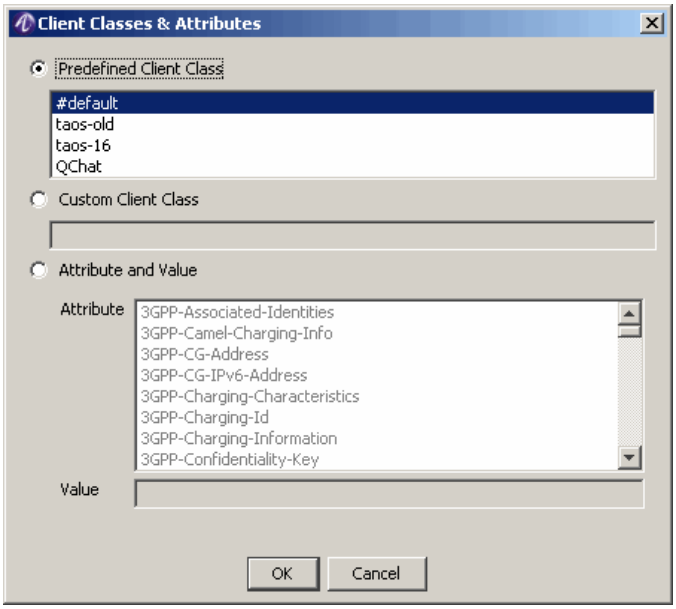
Figure 5-5 The Lucent Clients Dialog-Add record panel



This panel allows you to select the type of the Alcatel-Lucent client. Select the required client and select the configuration options for that type of client and click OK. The appropriate predefined client class is selected.

2. The **Insert a record** action button displays the **Client Classes and Attributes** dialog, Figure 5-6.

Figure 5-6 The Client Classes and Attributes dialog-Add record panel



3. This panel allows you to select the Client Classes and Attributes from either a list of Predefined Client Class, or allows you to add a Custom Client Class, or allows you to select/add the Attribute and value from the list.
4. The other action buttons in this panel allows you to perform the other required actions on the record(s).

Using the Comment tab in Radius Client Properties panel

The **Comment** tab is one of the tabs in the **Radius Client Properties** Panel. This tab allows you to add any comments about the **Radius Client Properties** panel.

The Diameter Peers tab

Diameter Peers tab

The **Diameter Peers** tab displays information about Diameter Peers in different columns.

Table 5-3 displays the **Diameter Peers** tab information.

Table 5-3 Client/Peers SMT-Diameter Peers tab Properties

Column Name	Description
Peer Name	Host name of the peer system to which the current reply server interacts.
Server Address	The Host IP Address.

Table 5-3 Client/Peers SMT-Diameter Peers tab Properties

Column Name	Description
Admin State	The state of the diameter server.
Tls	The Transport Layer Security (TLS). This is to secure the diameter server.
Client Classes and Attributes	The names for additional attributes. This includes Client Classes and other dictionary attributes and values. This section shows the names of any Client Classes to which this client has been assigned. In addition, any properties (specific Attribute Value Pairs (AVPs) assigned to the client are displayed. If it contains #default then there are no assigned classes or attributes for the client.

To go to the **Peer Entry** panel, click on the  action button. The **Peer Entry** panel is displayed as shown in Figure 5-7. This panel allows you to add records to the **Diameter Peers** or the **Peer Properties** panel. The **Peer Entry** panel, as shown in Figure 5-7, has the following three tabs:

- The **Peer Properties** tab that allows to add a record
- The **Client Classes and Attributes** tab that allows to select the required client option
- The **Comment** tab that allows to enter necessary comments

Using the Peer Properties tab to Add a record

The **Peer Properties** tab allows you to add a record and enter information in the required fields as shown in Figure 5-7.

Figure 5-7 The Peer Properties panel

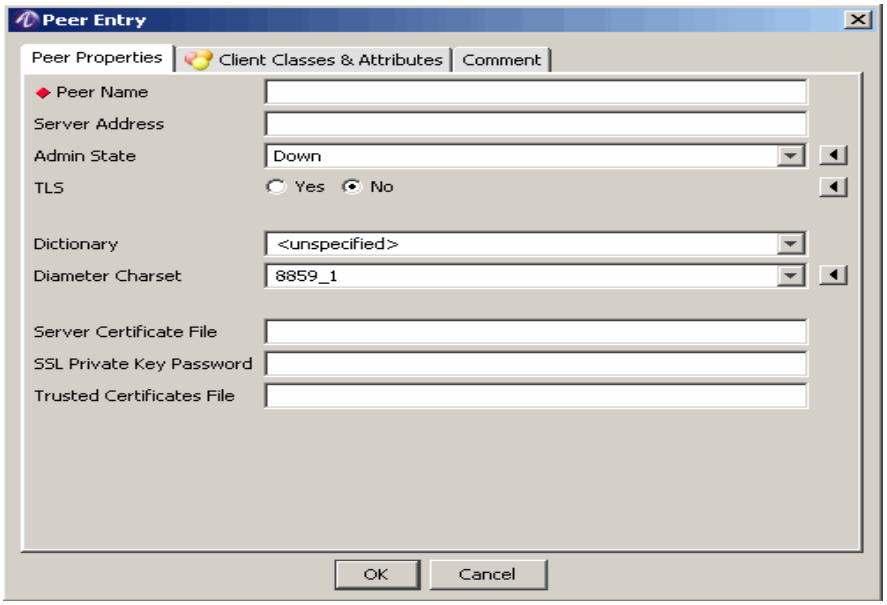


Table 5-8 explains each of these fields and the field descriptions.

Figure 5-8 Peer Properties panel-Properties

Field Name	Description
Peer Name	Specifies the name of the peer.
Server Address	Specifies the fully qualified domain name or the IP address of the peer.
Admin State	Specifies the admin state for the peer.
TLS	Yes or No option. Select Yes to encrypt the packets.
Dictionary	Specifies the dictionary name to use for this client class definition.
Diameter Charset	Specifies the default character set to use for character based Diameter AVP values which are lacking a defined encoding.
Server Certificate File	Server Certificate File that is used to configure TLS parameters.
SSL Private Key Password	Specifies the SSL Private Key Password used to secure connections over RMI. See SSL Configuration of the Server Properties panel for more information.
Trusted Certificates File	Trusted Certificates File that are used to configure TLS parameters.

Using the Client Classes & Attributes tab in the Peer Entry panel

The **Client Classes & Attributes** is one of the tabs in the **Peer Entry** Panel. This panel allows you to perform the following actions using the action buttons:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

1. The **Insert a record** action button displays the Client **Classes and Attributes** panel. This panel allows you to select the Client Classes and Attributes from either a list of Predefined Client Class, or allows you to add a Custom Client Class, or allows you to select/add the Attribute and value from the list.
2. The other action buttons in this panel allows you to perform the other required actions on the record(s).

Using the Comment tab in the Peer Entry panel

The **Comment** tab is one of the tabs in the **Peer Entry** Panel. This tab allows you to add any comments about the **Peer Entry** panel.

The TACACS+ Clients tab

TACACS+ Clients tab

The **TACACS+ Clients** tab displays information about TACACS+ Clients in different columns.

Table 5-4 displays the **TACACS+ Clients** tab information.

Table 5-4 TACACS+ Clients tab-Properties

Column Name	Description
Client IP Address or Host	The client IP address, range of IP address, host name, Fully Qualified Domain Name (FQDN), or Classless Inter Domain Routing (CIDN) block address. CIDN is another format of writing IP address.

Table 5-4 TACACS+ Clients tab-Properties

Column Name	Description
Shared Secret	The secret key shared between the 8950 AAA server and the client. The shared secret must be entered exactly the same way on both the 8950 AAA and the client. Errors in entering the secret key is one of the most common causes of 8950 AAA configuration problems.
Client classes & Attributes	This section shows the names of any Client Classes to which this client has been assigned. In addition, any properties (specific Attribute Value Pairs (AVPs) assigned to the client are displayed. If it contains #default then there are no assigned classes or attributes for the client.

To go to the **TACACS+ Client Properties** panel, click on the  action button. The **TACACS+ Client Properties** panel is displayed as shown in Figure 5-9. This panel allows you to add records to the **TACACS+ Clients** panel. The **TACACS+ Client Properties** panel, as shown in Figure 5-9, has the following three tabs:

- The **TACACS+ Client Properties** tab that allows to add a record
- The **Client Classes and Attributes** tab that allows to select the required client option
- The **Comment** tab that allows to enter necessary comments

Using the TACACS+ Client Properties tab to Add a record

The **TACACS+ Client Properties** tab allows you to add a record and enter information in the required fields as shown in Figure 5-9.

Figure 5-9 The TACACS+ Client Properties panel

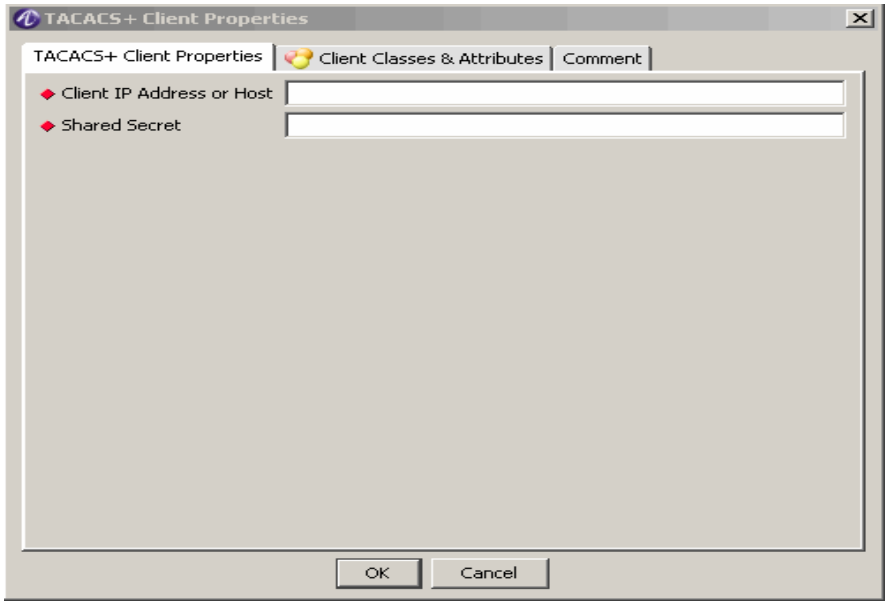


Table 5-10 explains each of these fields and the field descriptions.

Figure 5-10 TACACS+ Client Properties panel-Properties

Field Name	Description
Client IP Address or Host	Specifies the Domain name, IP Address, range of IP addresses, or a CIDR block of addresses.
Shared Secret	Shared secret between Policy server and client.

Using the Client Classes & Attributes tab in the TACACS+ Client Properties panel

The **Client Classes & Attributes** is one of the tabs in the **TACACS+ Client Properties** Panel. This panel allows you to perform the following actions using the action buttons:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

1. The **Insert a record** action button displays the Client **Classes and Attributes** panel. This panel allows you to select the Client Classes and Attributes from either a list of Predefined Client Class, or allows you to add a Custom Client Class, or allows you to select/add the Attribute and value from the list.
2. The other action buttons in this panel allows you to perform the other required actions on the record(s).

Using the Comment tab in the TACACS+ Client Properties Entry panel

The **Comment** tab is one of the tabs in the **TACACS+ Client Properties** Panel. This tab allows you to add any comments about the **TACACS+ Client Properties** panel.

The Client Classes tab

Client Classes tab

The **Client Classes** tab displays information about Client Classes in different columns.

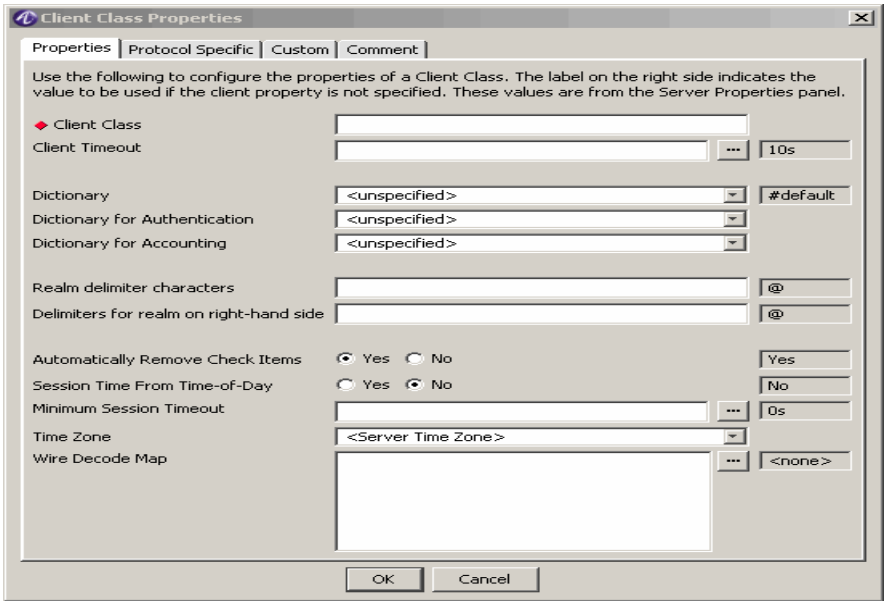
Table 5-11 displays the **Client Classes** tab information.

Figure 5-11 Client Classes tab-Properties

Column Name	Description
Client Class	The alias name for the client definition class.
Dictionary	Specifies the dictionary name to use for this client class definition.
Time Zone	Time zone where the NAS client is located.
Client Timeout	Time in milliseconds, to specify the amount of time the Policy server will wait before it discards the requests. This should match the timeout set on your NAS client.

To go to the **Client Class Properties** panel, click on the  action button. The **Client Class Properties** panel is displayed as shown in Figure 5-12.

Figure 5-12 The Client Class Properties panel-Properties tab



This panel has four tabs as following:

- Properties tab
- Protocol Specific tab
- Custom tab
- Comment tab

Using the Properties tab in the Client Class Properties

In the **Client Class Properties** panel, by default, the **Properties** tab is displayed as shown in Figure 5-12.

The **Properties** tab is used to configure the properties of a Client Class. The label on the right side indicates the value to be used if the client property is not specified. These values are from the Server Properties panel.

Table 5-5 explains each of the fields and field descriptions that are displayed in the Properties panel.

Table 5-5 Client Classes tab information

Field Name	Description
Client Class	The alias name for this client class definition.
Client Timeout	Time, in milliseconds, to specify the amount of time the Policy server will wait before it discards the requests. This should match the timeout set on your NAS client.

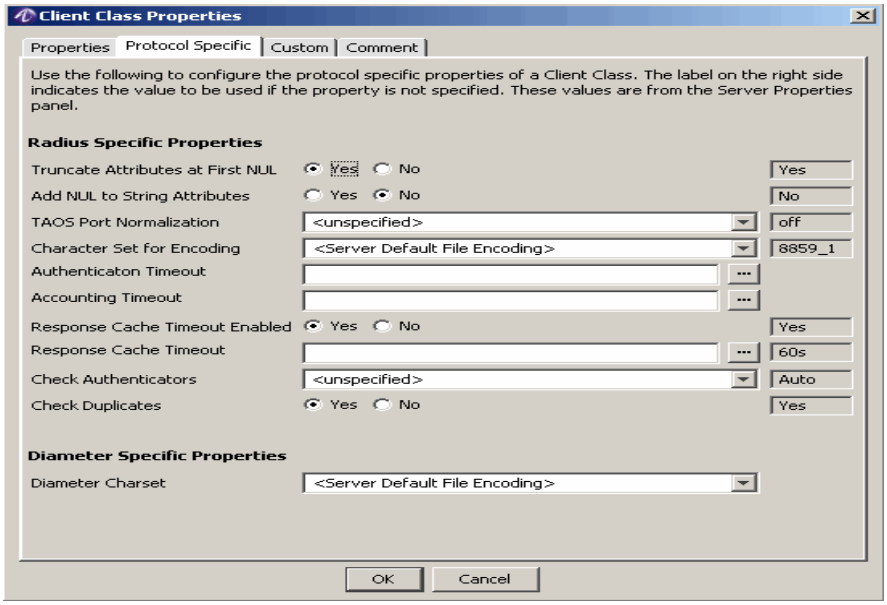
Table 5-5 Client Classes tab information

Field Name	Description
Dictionary	Specifies the dictionary name to use for this client class definition.
Dictionary for Authentication	Specifies the dictionary to use for authentication requests. This overrides the Client Dictionary value for authentications only.
Dictionary for Accounting	Specifies the dictionary to use for accounting records. This overrides the Client Dictionary value for accounting only.
Realm delimiter characters	List of characters in search order to parse the user name into a user and realm. By default, the realm is the left hand value and the user is the right hand value, unless the delimiter is found in the 'Delimiters for realm on right side' value. The default when not specified is '/@'.
Delimiters for realm on right-hand side	List of characters that mean the realm is the right hand value and the user is the left hand value of the parsed user name. This list should be a subset of the Realm Delimiter characters. The default when not specified is '@'.
Automatically Remove Check Items	Yes or No option. If enabled, the Policy server removes Check Items as they are checked by plug-ins.
Session Time From Time-of-Day	Yes or No option. If enabled, the session time is the time remaining from the Time-of-Day check item.
Minimum Session Timeout	The Policy server will reject any request that has a session-Time value less than the value specified by the property. If reply.Session-Time is not set then no action is needed.
Time Zone	Time zone where the NAS client is located.
Wire Decode Map	Specifies how to read the request from the wire (decode) into the Policy server. If not specified, '${request.*}:=${*};' is used.

Using the Protocol Specific tab in the Client Class Properties

To configure the **Protocol Specific** properties of a Client Class, click on the **Protocol Specific** tab in the **Client Class Properties** panel. The **Protocol Specific** tab is displayed as shown in Figure 5-13.

Figure 5-13 The Client Class Properties-Protocol Specific tab



The **Protocol Specific** tab is used to configure the protocol of a Client Class. The label on the right side indicates the value to be used if the property is not specified. These values are from the Server Properties panel.

Table 5-14 explains each of the fields and field descriptions that are displayed in the Protocol Specific tab.

Figure 5-14 The Client Class Properties-Properties tab information

Field Name	Description
Radius Specific Properties	
Truncate Attributes at First NUL	Yes or No option. If enabled, attributes are truncated at the first NUL found in the value. If disabled, the attribute values are not truncated. This enables support for NAS devices that send NUL characters in their attributes.
Add NUL to String Attributes	Yes or No option. If enabled, a NUL is appended to the end of plain string attributes in response requests to the NAS. This enables support for NAS devices that send NUL characters in their attributes.

Figure 5-14 The Client Class Properties-Properties tab information

Field Name	Description
TAOS Port Normalization	Specifies how to get the real NAS port number out of the NAS port info. This should only be used if your NASs are running TAOS.
Character Set for Encoding	Specifies the character set to use to encode string attributes in requests.
Authentication Timeout	Specifies the time, in milliseconds, the Policy server will wait before it discards authentication requests. This overrides the Client Timeout value for authentications only.
Accounting Timeout	Specifies the time, in milliseconds, the Policy server will wait before it discards accounting requests. This overrides the Client Timeout value for accounting requests only.
Response Cache Timeout Enabled	Yes or No option. If enabled, the Policy server caches responses for the time specified in the corresponding timeout property. If not enabled, responses are not cached.
Response Cache Timeout	When responding to RADIUS requests, the Policy server can remember (cache) the responses. If the response is sent, but lost and the NAS resends the same request, the Policy Server can respond with the cached response and not have to process the request again. This property sets how long the Policy Server keeps cached entries before discarding them.
Check Authenticators	If enabled, the Policy server checks the request authenticator and if not verified, the request is dropped.
Check Duplicates	Yes or No option. If enabled, the server checks to see if the request received is a duplicate of a previously received request. Duplicates are detected by a combination of the Source IP, Source Port, and Packet Authenticator. The default setting is true. This property can be set on a pre-client basis in the Client Properties.
Diameter Specific Properties	

Figure 5-14 The Client Class Properties-Properties tab information

Field Name	Description
Diameter Charset	Specifies the default character set to use for character based Diameter AVP values which are lacking a defined endcoding.

Using the Custom tab in the Client Class Properties

To use the other client attributes or customized properties of a Client Class, click on the **Custom** tab in the **Client Class Properties** panel.

The **Custom** tab is displayed with a set of action buttons under the **Other Client Attributes** section.

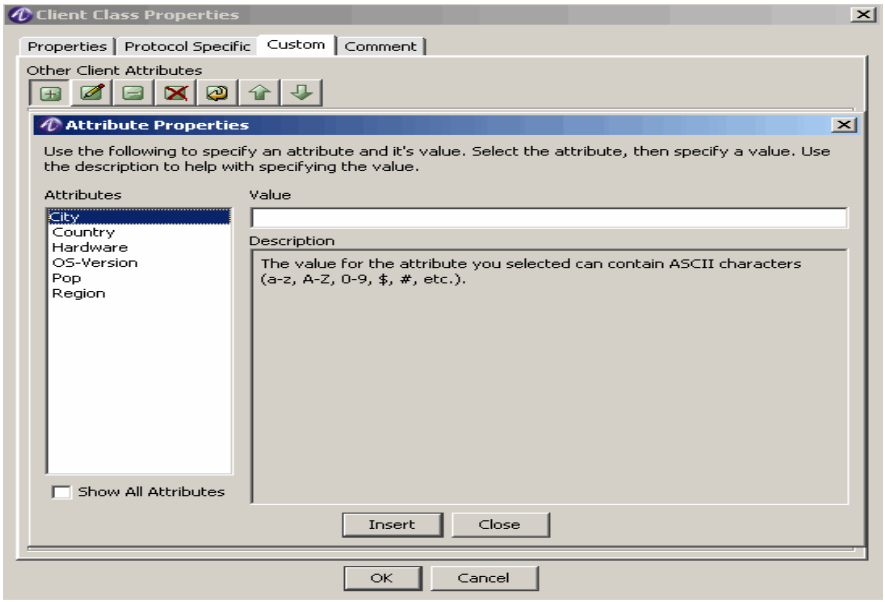
The **Custom** tab also allows you to perform the following actions using the action buttons:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

To add or Insert a record to the **Client Class Properties** panel, click on the  action button. The **Attribute Properties** panel is displayed as shown in Figure 5-15.

Figure 5-15 The Client Class Properties-Custom tab



The **Attribute Properties** panel allows you to specify an<Product Family> attribute and it’s value. Select the attribute, then specify a value. Use the description to help with the specifying the value.

Using the Comment tab in the Client Class Properties panel

The **Comment** tab is one of the tabs in the **Client Class Properties** Panel. This tab allows you to add any comments about the **Client Class Properties** panel.

END OF STEPS

6 Configuring 8950 AAA Realm Routing Table Properties

Overview

Purpose

This chapter discusses the process of configuring the Realm Routing Table.

The following topics are included in this chapter:

Configuring Realm Routing Table

Introduction

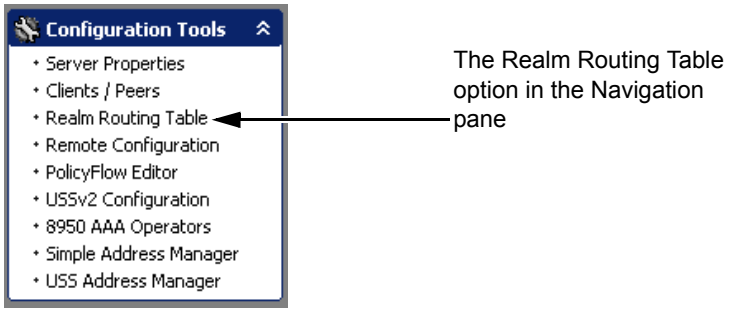
The Policy Server uses the entries in the Realm Routing table to determine how to route Diameter requests. The Policy Server uses the realm, Diameter application, vendor and packet type of the Diameter request to match Realm Route entries. Once a match is found, the request is routed locally, proxied, or redirected based on the Action in the entry.

Using the SMT to Configure Realm Routing Table

This section describes how to configure a 8950 AAA Realm Routing Table. The specific procedure that follows lists steps to configure or modify an existing Realm Routing Table using the Server Management Tool. For information about running the SMT, please refer to "Starting the Server Management Tool".

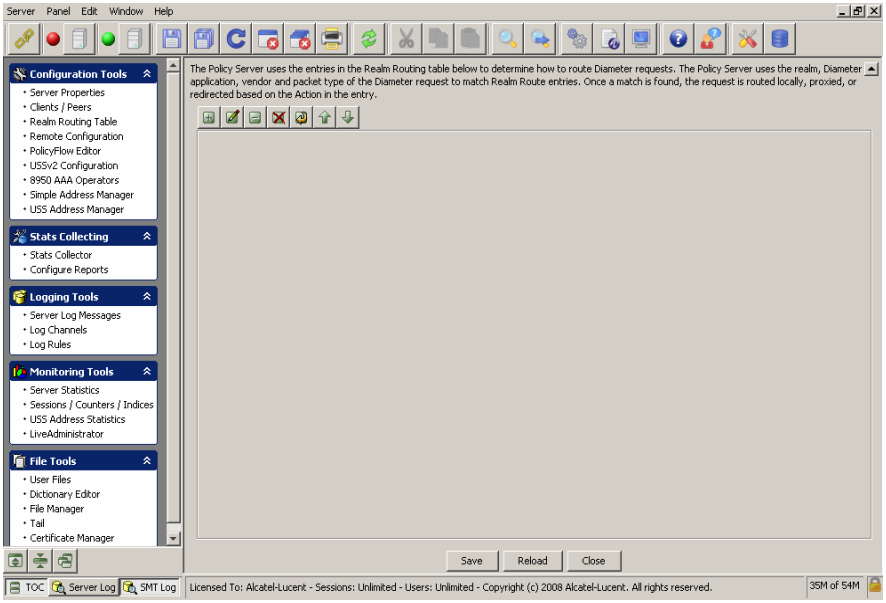
1. Select **Realm Routing Table** from the Configuration Tools folder on the Navigation pane, as shown in Figure 6-1.

Figure 6-1 Navigation Pane-Realm Routing Table option



Result: The 8950 AAA Realm Routing Table panel is displayed as shown in Figure 6-2.

Figure 6-2 The 8950 AAA SMT-Realm Routing Table panel



The **Realm Routing Table** panel (Figure 6-2) contains a menu bar that consists of a set of Action Buttons that appear at the top of the 8950 AAA Realm Routing Table panel, as shown in Figure 6-2.

The Action buttons are as shown in Figure 6-3.

Figure 6-3 Realm Routing Table-Action buttons

These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record

- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

To Insert a record, click on the  action button. The **Route Entry** panel is displayed as shown in Figure 6-4. This panel allows you to add a record and enter information in the required fields to the Realm Routing Table as shown in Figure 6-4.

Figure 6-4 The Route Entry-Add record panel

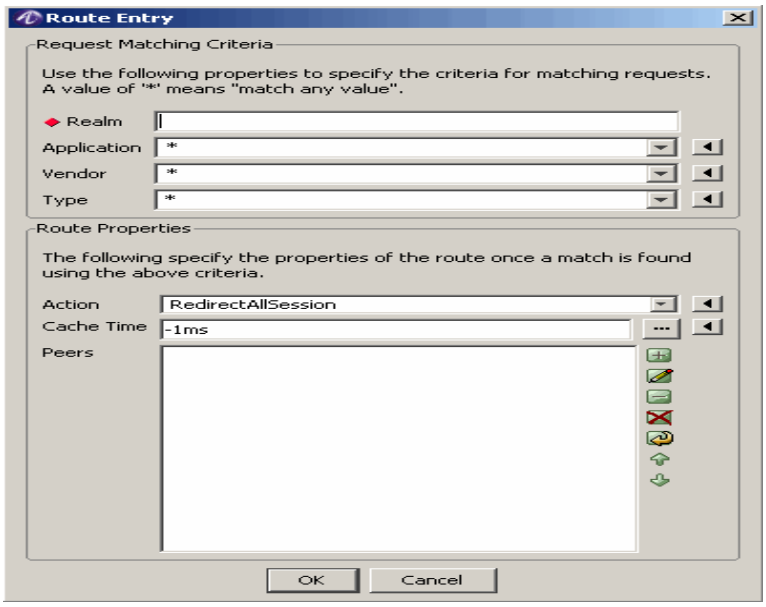


Table 6-1 explains each of these fields and the field descriptions. There are two sets of properties that you need to specify in this screen.

- The Request Matching Criteria

  This is used to specify the criteria for matching requests. A value of '*' means match any value.

- The Route Properties

  This is used to specify the properties of the route once a match is found using the above criteria.

Table 6-1 Route Entry Properties

Field Name	Description
Request Matching Criteria	
Realm	Specifies the realm name for which this route entry is valid.
Application	Specifies the application for which the route entry is valid. Valid values are the provided values, either '*' for any application or one of the application names. Application can also be entered as a numeric value which in addition enables entry of a Vendor identity.
Vendor	Specifies the vendor specific application id for which this route entry is valid when combined with the application ID. Valid values are any of the predefined from the list or a numeric value.
Type	Specifies the type. Can be either Authentication or Accounting.
Route Properties	
Action	Specifies the route action to take when all of application, vendor specific application id (if applicable) and realm name matches.
Cache Time	Specifies the value in seconds that the server provides in the "Redirect-Max-Cache-Time" attribute when the server sends a redirect indication based on a match of this entry.
Peers	When appropriate Action is selected, this field is activated. A list of action buttons are displayed next to this field, click on the required action button to perform the required action. If you click on the Insert a record action button, the Host window panel is displayed that allows you to add a **Host** to the selected **Peer**.

END OF STEPS

7 Configuring 8950 AAA Remotely

Overview

Purpose

This chapter discusses the process of configuring the 8950 AAA remotely.

The following topics are included in this chapter:

Remote Configuration

Introduction

The Remote Configuration feature allows you to retrieve files from a remote server using the Configuration Server.

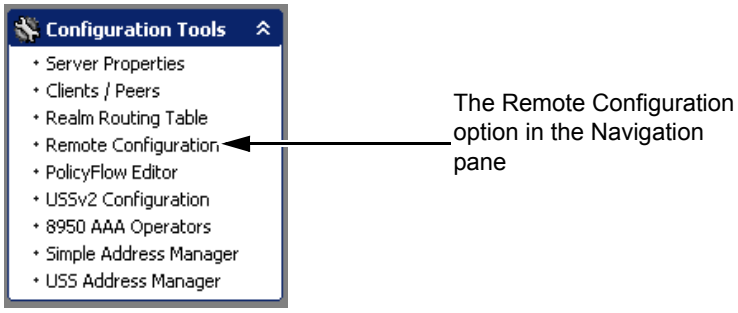
Using the SMT to retrieve files from a remote server

This section describes how to configure a 8950 AAA to retrieve files from a remote server. This is typically used to have one centralized location for configuration files. You must specify which files are retrieved for every Policy Server.

For information about running the SMT, please refer to “Starting the Server Management Tool”.

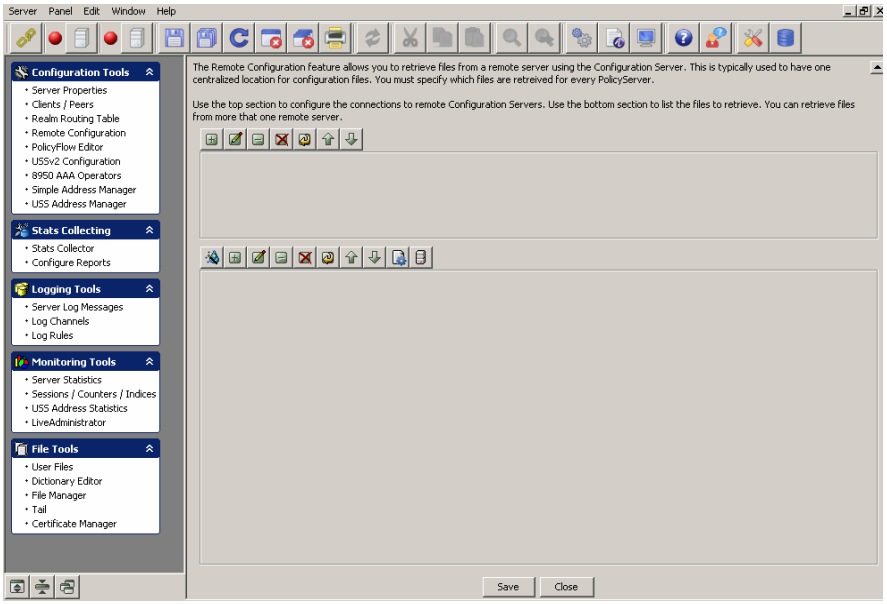
1. Select **Remote Configuration** from the Configuration Tools folder on the Navigation pane, as shown in Figure 7-1.

Figure 7-1 Navigation Pane-Remote Configuration option



Result: The **8950 AAA Remote Configuration** panel is displayed as shown in Figure 7-2.

Figure 7-2 The 8950 AAA SMT-Remote Configuration panel



Action buttons-Top Section

The **Remote Configuration** panel (Figure 7-2) contains two sections that consists of 2 sets of Action buttons that appear in the 8950 AAA Remote Configuration panel, as shown in Figure 7-2.

The action buttons that are in the top section are used to configure the connections to remote configuration servers. The action buttons that are in the bottom section are used to list the files to retrieve. You can retrieve files from more than one remote server.

The Top set of action buttons are as shown in Figure 7-3.

Figure 7-3 Remote Configuration-Action buttons in the top section

These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

To Insert a record, click on the  action button. The **Server Entry** panel is displayed as shown in Figure 7-4. This panel allows you to add a record and enter information in the required fields to specify a server entry as shown in Figure 7-4.

Figure 7-4 The Server Entry-Add record panel

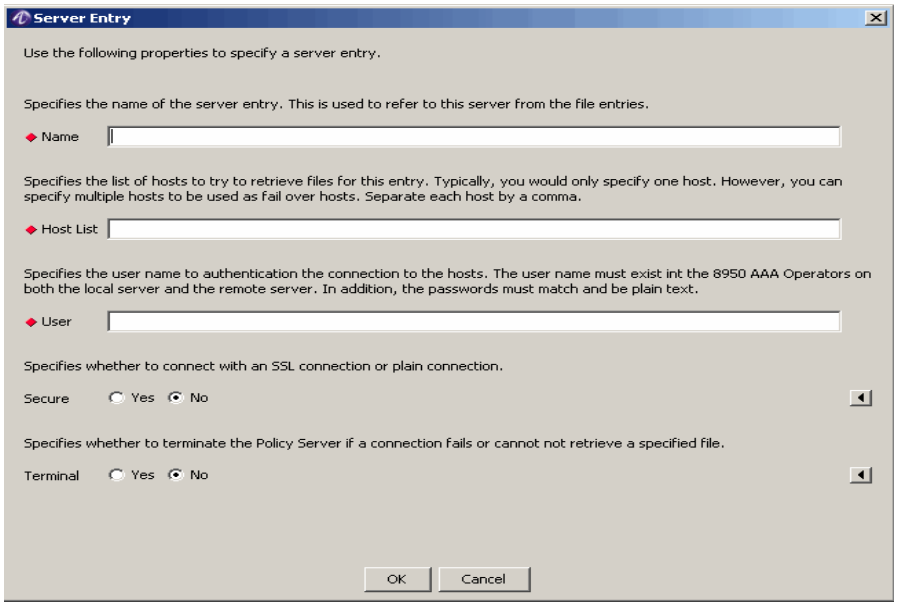


Table 7-5 explains each of these fields and the field descriptions that you need to specify in this screen.

Figure 7-5 Server Entry Properties

Field Name	Description
Name	Specifies the name of the server entry. This is used to refer to this server from the file entries.
Host List	Specifies the list of hosts to try to retrieve files for this entry. Typically, you would only specify one host. However, you can specify multiple hosts to be used to be used as fail over hosts. Separate each host by a comma.
User	Specifies the user name to authentication the connection to the hosts. The user name must exist in the 8950 AAA Operators on both the local server and the remote server. In addition, the passwords must match and be plain text.
Secure	Yes or No option. Specifies whether to connect with an SSL connection or plain connection.
Terminal	Yes or No option. Specifies whether to terminate the Policy Server if a connection fails or cannot retrieve a specified file.

Action buttons-Bottom Section

The action buttons that are in the bottom section are used to list the files to retrieve. You can retrieve files from more than one remote server.

The Bottom set of action buttons are as shown in Figure 7-6.

Figure 7-6 Remote Configuration-Action buttons in the bottom section

These action buttons allow you to perform the following actions:

- Insert Row Wizard
- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down
- Assigns a file format to the selected entry in the file table
- Click on this to get a list of available file formats. You can select any from the list.
- Assigns a server to the selected entry in the file table

  Click on this to get a list of available servers. You can select any from the list.

You can perform any of these required actions using these action buttons.

To Insert a record, click on the  action button. The **File Entry** panel is displayed as shown in Figure 7-7. This panel allows you to add a record and enter information in the required fields to specify a server entry as shown in Figure 7-7.

Figure 7-7 The File Entry-Add record panel

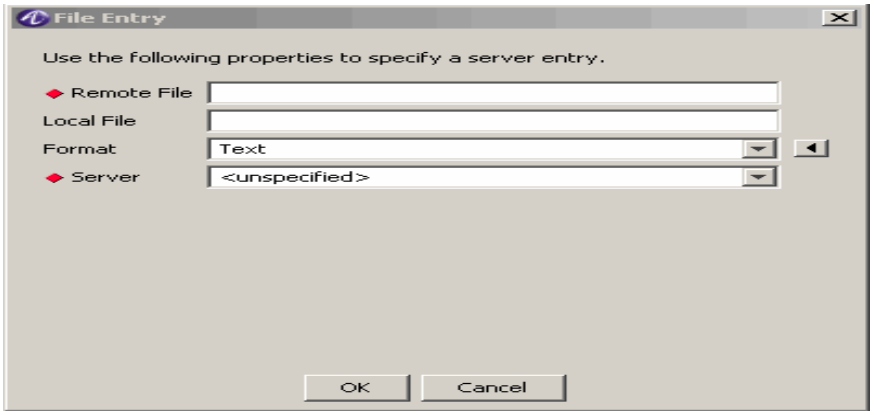


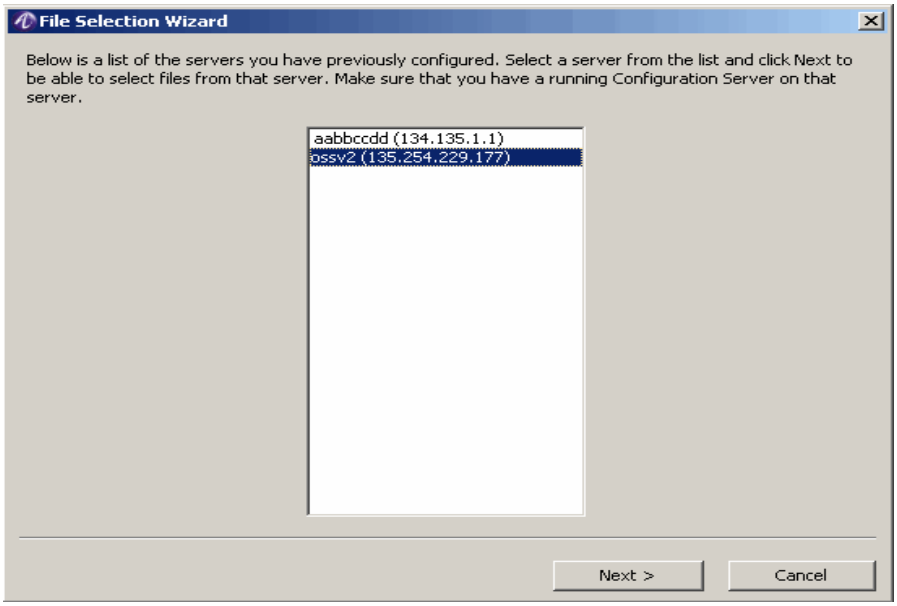
Table 7-8 explains each of these fields and the field descriptions that you need to specify in this screen.

Figure 7-8 File Entry Properties

Field Name	Description
Remote File	Specifies the name of the file from the remote server.
Local File	Specifies the name of the file to be saved locally. This can be a different name than the remote file name.
Format	Specifies the format of the file.
Server	Specifies the server configuration to use to retrieve the file.

To Insert Row Wizard, click on the  action button. The **File Selection Wizard** panel is displayed as shown in Figure 7-9.

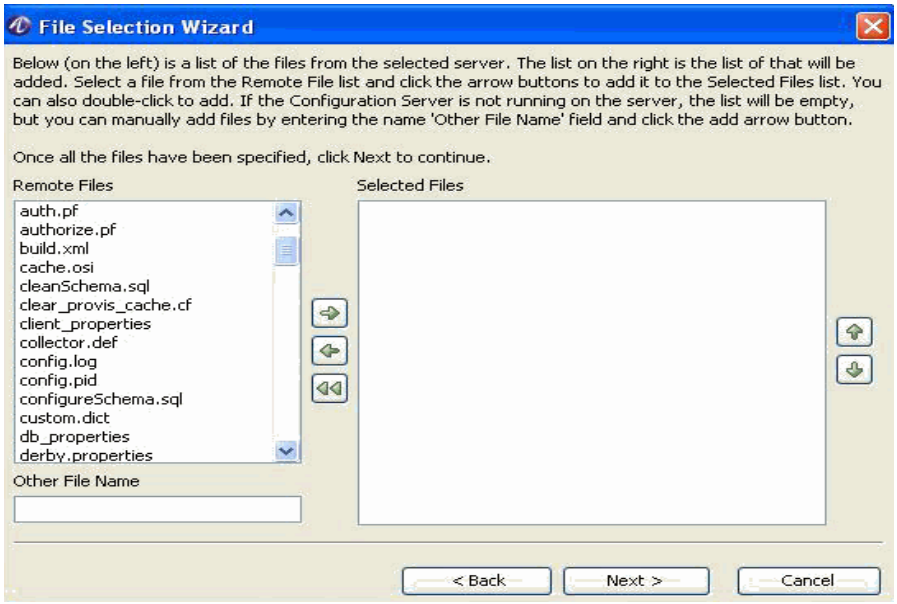
Figure 7-9 The File Selection Wizard panel



This panel displays a list of the servers you have previously configured. Select a server from the list and click **Next** to be able to select the Remote files.

The **File Selection Wizard** panel is displayed as shown in Figure 7-10.

Figure 7-10 The File Selection Wizard panel



This panel displays a list of files from the selected server. The list on the right is the list of that will be added. Select a file from the Remote File list and click the arrow buttons to add it to the Selected Files list. You can also double-click to add. If the Configuration Server is not running on the server, the list will be empty, but you can manually add files by entering the name ‘Other File Name’ field and click the add arrow button.

Once all the files have been specified, click **Next** to continue.

END OF STEPS

8 Using the 8950 AAA Policy Flow Editor

Overview

Purpose

This chapter discusses the process of configuring and creating necessary entities for the Policy Flow Editor in the 8950 AAA Server Management Tool.

The following topics are included in this chapter:

Policy Flow Editor

How to install the Policy Flow Editor

You can elect to install the PolicyFlow Editor during the 8950 AAA installation process. If you see the *PolicyAssistant* in the Navigation Pane and do not see the PolicyFlow Editor, then the PolicyFlow Editor is not installed.

The procedure for installing the PolicyFlow Editor using the SMT is described in the "Installing the PolicyAssistant and the Policy Flow Editor" section of Chapter 3, "Server Management Tool Command Set,". Refer to this section/chapter for more information.

Introduction

The following sections describe how to configure the 8950 AAA PolicyFlow Editor.

The PolicyFlow Editor panel has three sections, the top section, middle section, and the bottom section. You need to perform necessary actions in the following order to create and associate a PolicyFlow file.

- The middle section, the Policy Flow Section, is used to create the policy flows.

  Use the Policy Flow section to create policies. This is the first step that you need to perform.

- The bottom section, is used to manage the Method configuration entities for the policy flows.

  Use the Method Configuration section to define the methods to emulate your business model of how authenticate, authorize users and deal with session accounting and information.

  This is the second step you need to perform.

- The top section which is the Method Dispatch section is used to determine how to route requests to the policy flows that are defined in the bottom section.

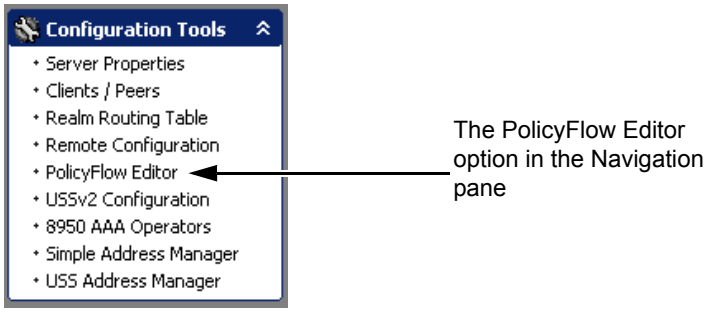
  Use the Method Dispatch section to define entries that match requests with specific protocols such as RADIUS, Diameter, TACACS+ as well as internal type matching for Cron and USS Triggers.

  This is the third step you need to perform.

For information about running the SMT, please refer to "Starting the Server Management Tool".

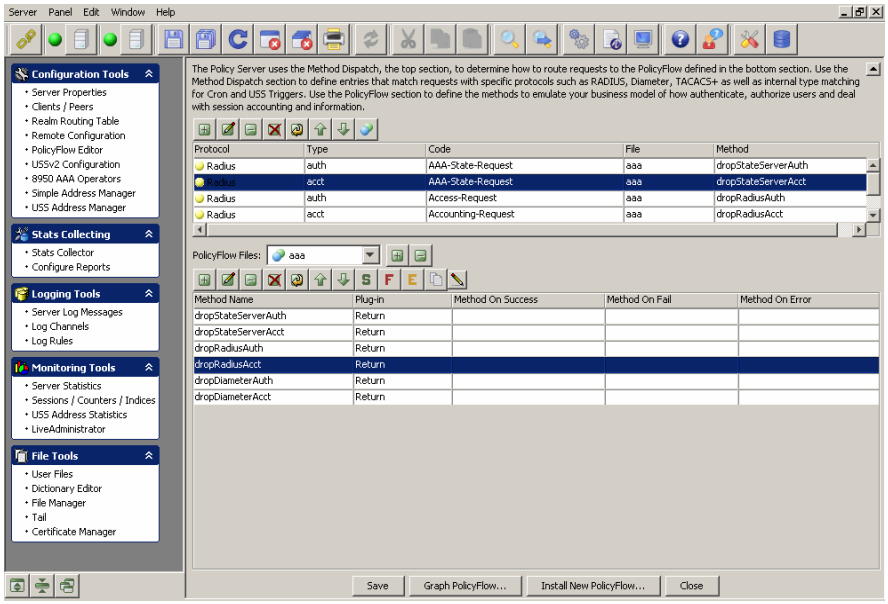
1. Select **PolicyFlow Editor** from the Configuration Tools folder on the Navigation pane, as shown in Figure 8-1.

Figure 8-1 Navigation Pane-Policy Flow Editor option



Result: The **8950 AAA PolicyFlow Editor** panel is displayed as shown in Figure 8-2.

Figure 8-2 The 8950 AAA SMT-PolicyFlow Editor panel



Policy Flow Files

Policy Flow Files Section

The Policy Flow Files section is the middle or in-between section of the PolicyFlow Editor panel.

This section is used to add or delete PolicyFlow Files. The Method Configurations that are defined and are associated with a PolicyFlow File are displayed just below this section after another set of action buttons in the bottom section.

The PolicyFlow Files section has two action buttons as shown in Figure 8-3.

Figure 8-3 PolicyFlow Editor-Action buttons in the PolicyFlow Files section

These action buttons allow you to perform the following actions:

- Insert a PolicyFlow file
- Delete a PolicyFlow file

The action button, +, allows you to add a new PolicyFlow file. When you click the + action button, you get a pop-up window that will ask you to enter the name of the new file. Enter the name and click **OK** to add the new entry. You can see the new entry in the PolicyFlow Files drop-down list box.

The other action button, -, allows you to delete the selected PolicyFlow file. Select the required PolicyFlow file from the drop-down list box and click the - action button. A pop-up window will ask you if you are sure you want to delete the selected PolicyFlow File. Click **Yes** to delete or **No** to not delete and come out.

Method Configuration

Method Configuration Section

The Method Configuration section is the last section or the bottom section of the PolicyFlow Editor panel. This is used to manage the Method configuration entities of the PolicyFlow Editor.

A set of action buttons, as shown in Figure 8-4, are in this section of the panel that are used to create and define the Method Dispatch properties.

Figure 8-4 PolicyFlow Editor-Action buttons in the Method Configuration section

These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down
- Assign Method On Success of selected method
- Assign Method on Failure of selected method
- Assign Method on Error of selected method
- Copy a method from another method file
- Click to enter/edit the comments for the methods file

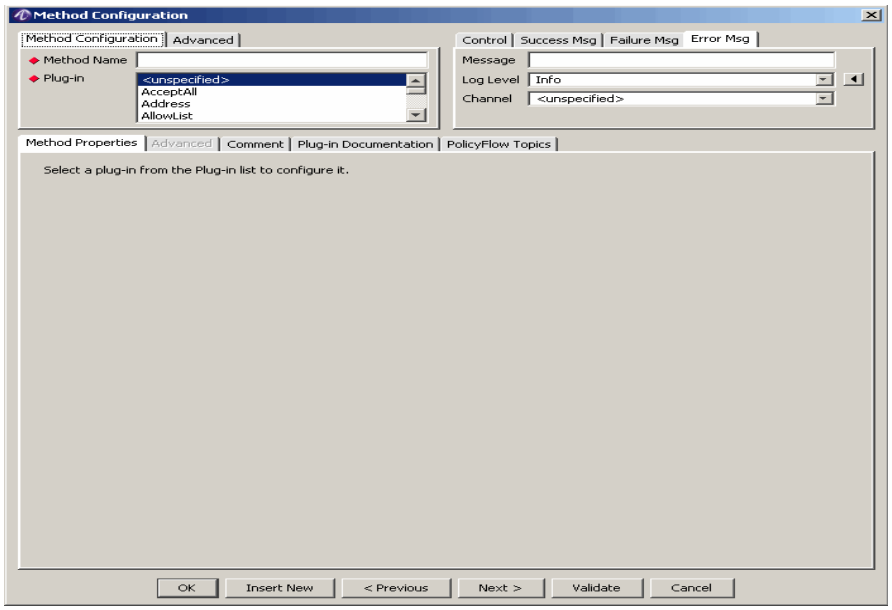
You can perform any of the required actions using these action buttons.

Important! Some of the necessary actions will be available with some of these buttons. Any available actions are displayed for you to choose when you right click on the action buttons.

Important! To copy a method under a PolicyFlow file from another method file, right click on the Copy a method from another method file icon. Select the desired method from the policyflow file list. The method gets added in the selected policyflow file. You can also rename an existing method under the a policyfile.

1. To go to the **Method Configuration** panel, click the  action button. The **Method Configuration** panel is displayed as shown in Figure 8-5. This panel allows you to add or insert records to the Method Configuration.

Figure 8-5 PolicyFlow Editor-Method Configuration panel



The **Method Configuration** panel, as shown in Figure 8-5, has three sections.

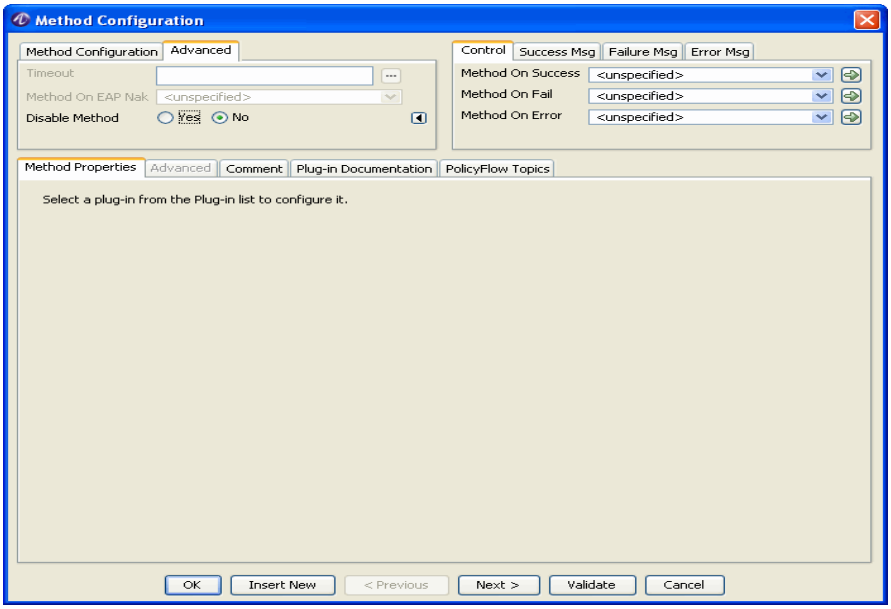
- The first section that has two tabs: the Method Configuration tab and the Advanced tab. Both these tabs allow you to define the properties for the method configuration fields that are displayed.
- The second section that has 4 tabs: the Control tab, the Success Msg tab, the Failure Msg tab, and the Error Msg tab. These tabs allow you to define the properties for the method configuration fields that are displayed.
- The third section that has five tabs: the Method Properties tab, the Advanced tab, the Comment tab, the Plug-in Documentation tab, and the PolicyFlow Topics tab. By default, the Method Properties tab is activated/displayed. This section displays the Method Properties of the Method Name and Plug-in that is selected.

The **Method Configuration** tab, as shown in Figure 8-5, allows you to enter the method name and the plug-in to be used for the method.

Use the **Advanced** tab to specify the additional method attributes as shown in Figure 8-6.

Use the Timeout field to enter the timeout duration. Timeout specifies the maximum time that a particular plug-in takes before following an error path. Method On EAP Nak specifies the method to be invoked when the specified plug-in receives an EAP Nak from the client. If the plug-in receives an EAP Nak and the Method On EAP Nak is unspecified then, the plug-in follows an error path. Disabled Method, if set true, does not allow the server to use the specified method.

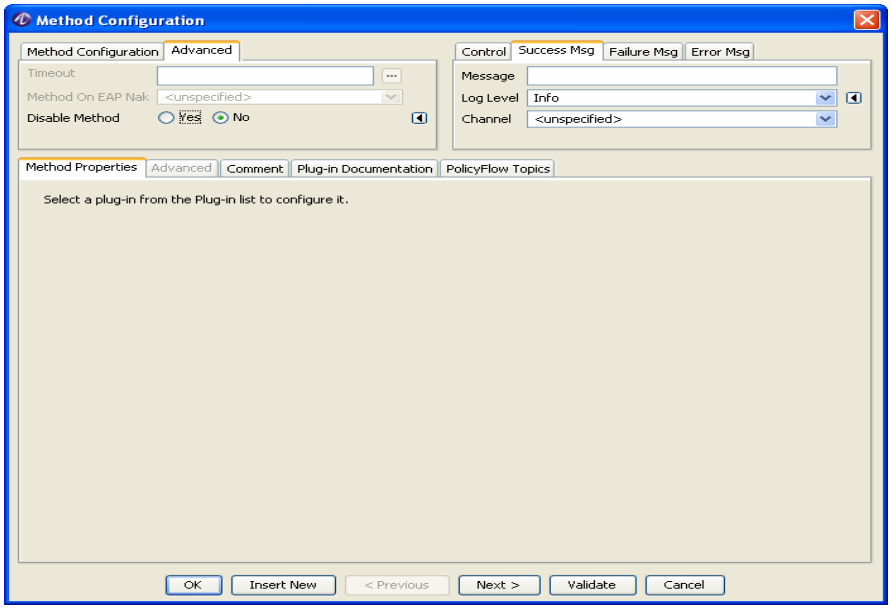
Figure 8-6 Method Configuration pane - Advanced tabl



Use the **Control tab** allows you to control the methods during the progress of plug-in as shown in the Figure 8-6. Use the **Method On Success** of Control tab to specify the method to be invoked when the plug-in completes successfully. If left unspecified, the request is considered to be accepted. **Method On Fail** is used to specify the method to be invoked when the plug-in fails. If left unspecified, the request is considered to be rejected. **Method On Error** is used to specify the method to be invoked when the plug-in encounters an error.

Use the **Success Msg**, **Failure Msg**, and **Error Msg** tabs to specify the message, log level, and channel if the specified method succeeds, fails or encounters an error respectively (see Figure 8-7).

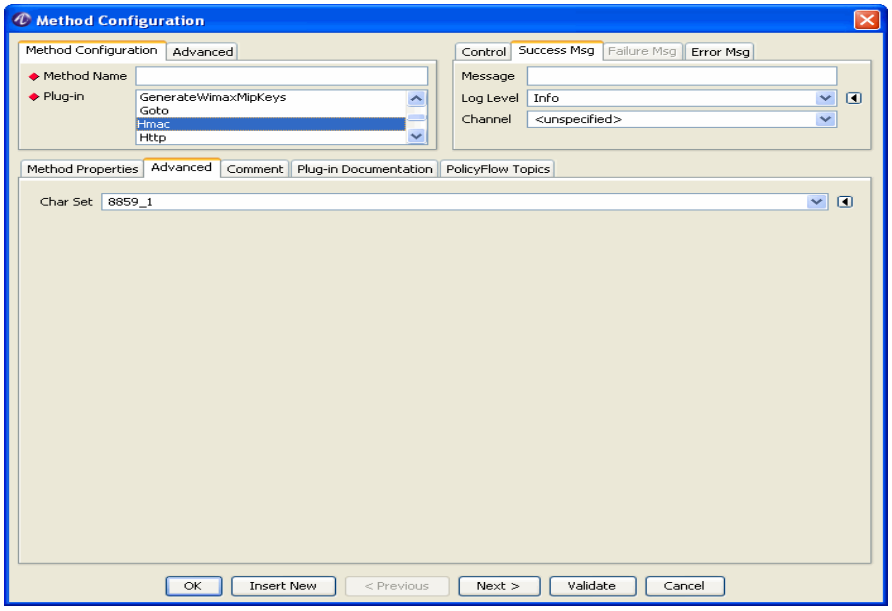
Figure 8-7 Method Configuration pane - Success Msg tabl



Use the **Method Properties** tab to specify the properties of the method chosen as shown in the Figure 8-7.

Advanced tab allows you to specify additional properties of the some of the methods (methods which have additional attributes) as shown in the Figure 8-8.

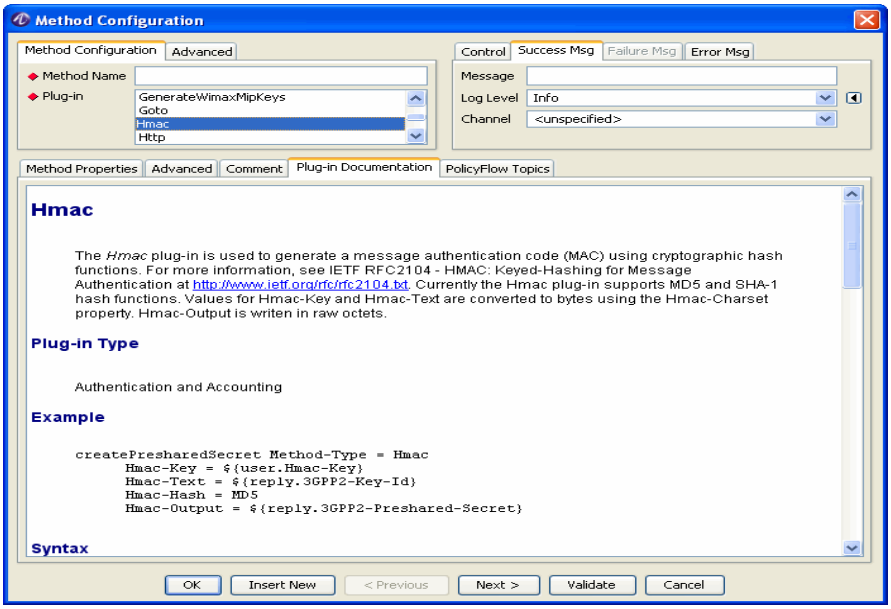
Figure 8-8 Method Configuration pane - Success Msg tabl



Use **Comments** tab to enter your comments, if any.

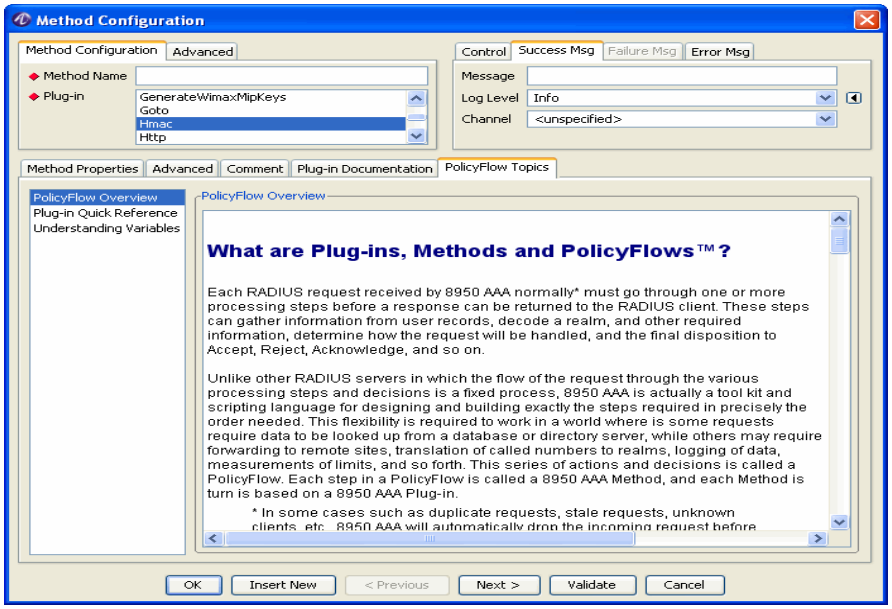
The **Plug-in Documentation** provides you the details the plug-in chosen (see Figure 8-9).

Figure 8-9 Method Configuration pane - Success Msg tabl



PolicyFlow Topics tab describes in general about the plug-ins, methods, and the policyflow along with their properties (see Figure 8-5).

Figure 8-10 Method Configuration pane - Success Msg tabl



Method Dispatch Section

Method Dispatch Section

The Method Dispatch section is the top section of the PolicyFlow Editor panel. This is used to determine how to route requests to the PolicyFlows that are defined in the bottom section.

One set of action buttons, as shown in Figure 8-11, are in the Method Dispatch section of the panel that are used to define the Method Dispatch properties.

Figure 8-11 PolicyFlow Editor-Action buttons in the Method Dispatch section

These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

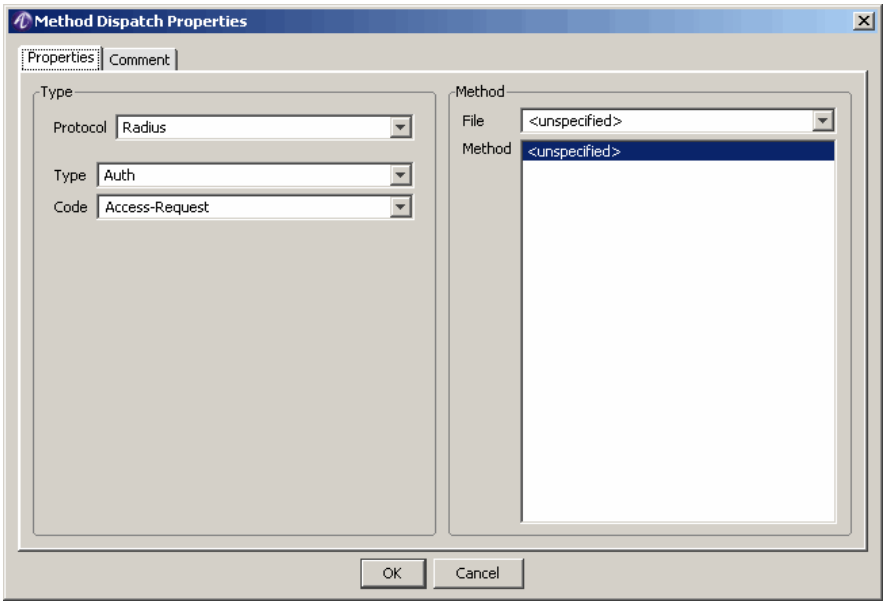
- Assign File and Method for selected row

You can perform any of the required actions using these action buttons.

Important! Some of the necessary actions will be available with some of these buttons. Any available actions are displayed for you to choose when you right click on the action buttons.

1. To go to the **Method Dispatch Properties** panel, click the  action button. The **Method Dispatch Properties** panel is displayed as shown in Figure 8-12. This panel allows you to add or insert records to the Method Dispatch Properties.

Figure 8-12 PolicyFlow Editor-Method Dispatch Properties panel



The **Method Dispatch Properties** panel, as shown in Figure 8-12, has two tabs:

- The Properties tab that allows to add a record.
- The Comment tab that allows to enter necessary comments.

By default, the **Properties** tab is activated and this tab allows you to enter the Method Dispatch Properties tab details.

Table 8-13 explains each of these fields and the field descriptions that appear in the Properties Tab of the **Method Dispatch Properties** Panel.

Figure 8-13 Method Dispatch Properties-Properties tab

Field Name	Description
Type	
Protocol	Specifies the protocol: radius, diameter, USS trigger, TACACS+, or cron.

Figure 8-13 Method Dispatch Properties-Properties tab

Field Name	Description
Type	Specifies the packet type.
Code	Specifies the code point of packet type.
Method	
File	Specifies the name of the method file that contains the method to start processing PolicyFlow.
Method	Specifies the name of the starting method in the file to start processing PolicyFlow.

2. To edit a **Method Dispatch Property,** select a required Protocol/method property from the **8950 AAA PolicyFlow Editor** panel, Figure 8-2, click the  action button. The **Method Dispatch Properties** panel is displayed with the selected record details. This panel allows you to edit the records in the Method Dispatch Properties.
3. The Delete Selected record action button, allows you to delete the selected record.
4. The Delete all records action button allows you to delete all the records in the panel.
5. The Make a copy of the selected record allows you to make a copy of a record and displays the selected record details in the Method Dispatch Properties panel and allows you to change any details too, if necessary, and make a copy of that record.
6. The Move selected record UP or Down action buttons allow you to move the record either up or down.
7. The Assign File and Method for selected row action button displays a list of Policy Flow Files and the Method names associated with the these files. It allows you to assign the required File name and method to the selected protocol.

END OF STEPS

9 Using the 8950 AAA Policy Assistant in Server Management Tool

Overview

Purpose

This chapter discusses the process of how to use, configure, and create necessary entities for the PolicyAssistant in the 8950 AAA Server Management Tool.

This chapter describes how to use the PolicyAssistant and Policy Wizard to create and access Policies.

The following topics are included in this chapter:

Understanding PolicyFlow, the PolicyAssistant, and the Policy Wizard

About PolicyAssistant and Policy Wizard

The PolicyAssistant is a tool for creating access policies. It provides an easy way to configure 8950 AAA software through its built-in *Policy Wizard.* The Policy Wizard collects data about how your requests should be processed and saves that data to special PolicyAssistant files.

The PolicyAssistant panel within the SMT is the starting point for using the Policy Wizard. This panel contains a table of available policies that you have defined for your network. Each policy defines the user source (where user profiles are stored), the type of authentication the server performs, user and policy limits, and how accounting information is processed. You use the Policy Wizard to create policies and populate this table. The first time you run the PolicyAssistant the table panel will not appear, instead the Policy Wizard will start automatically so you can create your first policy.

The Policy Wizard will help you define the following information for each policy you create:

- A name to be assigned to each policy you create.
- The location where user profiles will be stored (Files, LDAP, Database, and so on).
- The method used to authenticate users (text passwords, Secure Token cards, and so on).
- A set of rules for how accounting records are processed.
- Any session limits that might apply to this policy.

Installing the PolicyAssistant

How to install the Policy Assistant

You can elect to install the PolicyAssistant during the 8950 AAA installation process. If you see the *PolicyFlow Editor* in the Navigation Pane and do not see the PolicyAssistant, then the PolicyAssistant is not installed.

The procedure for installing the Policy Assistant using the SMT is described in the Installing the PolicyAssistant and the Policy Flow Editor section of Chapter 3, “Server Management Tool Command Set,”. Refer to this section/chapter for more information.

Preparing to Create Your First Policy

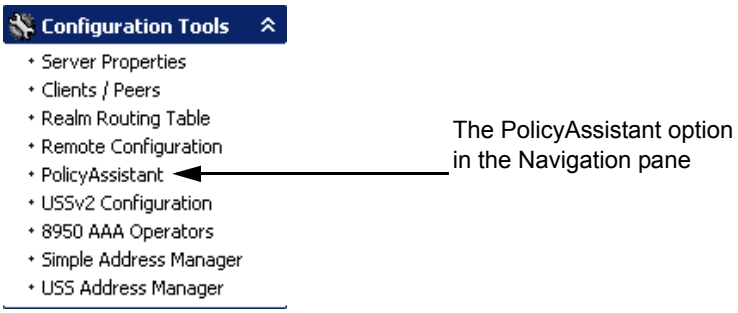
Opening the PolicyAssistant

The following sections describe how to configure the 8950 AAA PolicyAsssistant.

As explained earlier in Chapter 3, “Server Management Tool Command Set,” only one of the Policy functions, either the PolicyFlow Editor or PolicyAssistant, can be operated at a time. Please refer to this section/chapter to toggle between these two functions.

If you elect to work with the Policy Assistant panel and take the necessary actions, the Policy Assistant item is displayed in the Navigation pane under Configuration Tools as shown in Figure 9-1.

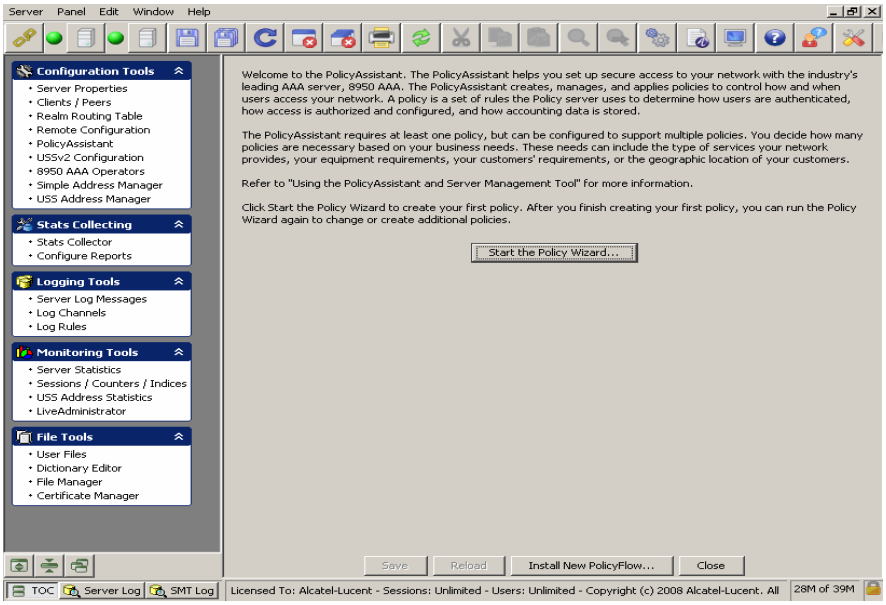
Figure 9-1 Navigation Pane-PolicyAssistant option



To open the Policy Assistant, click **PolicyAssistant** in the SMT Navigation pane as shown in Figure 9-1.

Result: The PolicyAssistant Welcome panel appears. If this is the first time you have accessed the PolicyAssistant (or if you have not previously saved a policy from this panel) you will see a Welcome message as shown in Figure 9-2.

Figure 9-2 PolicyAssistant Welcome Panel



Using the Policy Wizard

About Policy Wizard

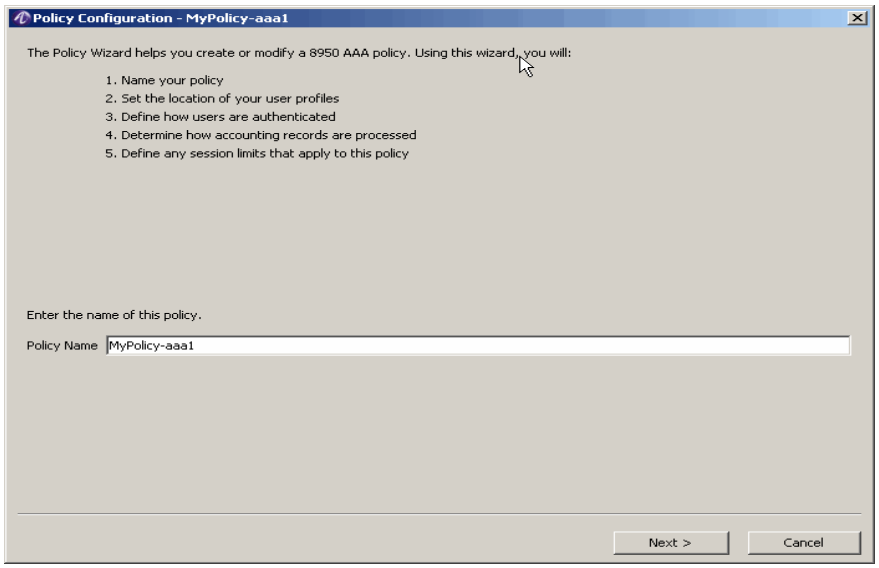
The following sections walk you through the primary functions addressed by the Policy Wizard.

Your first objective as a 8950 AAA administrator is to determine the components of your policy: how your network stores user profiles (user source), authenticates users (authentication source), applies access rules, set session parameters and processes accounting data. You must create a policy for each unique set these components. If you have multiple sets of these components, you must run the Policy Wizard multiple times to create a policy for each combination.

Naming Your Policies

When you click on the **PolicyAssistant** in the SMT Navigation pane, Figure 9-1, the PolicyAssistant Welcome panel appears as shown in Figure 9-2. Click on the **Start the Policy Wizard** button. The **Policy Configuration - MyPolicy** panel is displayed, as shown in Figure 9-3.

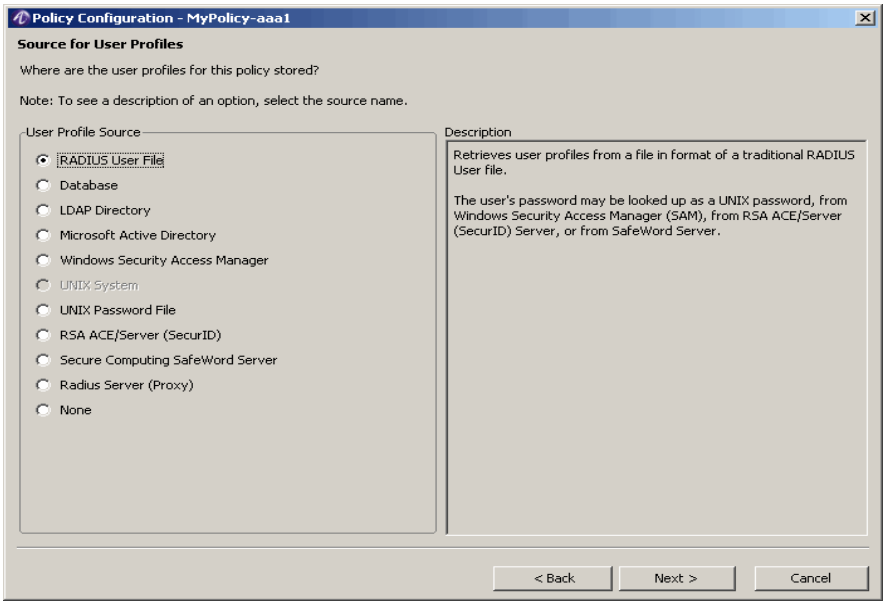
Figure 9-3 Policy Name Panel in the Policy Wizard



Enter a **Policy Name** for this policy that is descriptive of the configuration that it represents. A policy name helps you organize multiple policies. Examples of good policy names might be: Dial-Access-Policy, Wi-Fi-Policy, Proxy-Users, Sales-Department, etc.

Click **Next** to continue. The **Source for User Profiles** panel appears as shown in Figure 9-4.

Figure 9-4 Policy Configuration-Source for User Profiles panel in Policy Wizard



Select a **User Profile Source** from the list, as shown on the left side of the panel in Figure 9-4. A description of the source appears on the right-hand side of the panel when you select a source. Depending on the source you select, the Policy Wizard may require additional information later in the Policy Wizard.

The sections below provide additional information for the following supported user profile sources:

- RADIUS User Files
- Database
- LDAP Directory
- Microsoft Active Directory
- Windows Security Access Manager
- UNIX System
- RSA ACE/Server (SecurID)
- Secure Computing SafeWord Server
- Radius Server (Proxy)

RADIUS User Files

8950 AAA supports the use of traditional RADIUS user files. RADIUS user files are uniquely formatted text files. The Server Management Tool enables you to create and manage these files without the need to understand or implement the formatting rules.

A user file contains a user profile for each user who accesses your network. You may create your user file to function only as a user source (for authorization, and configuring a user session) or also as a source that provides information for authentication, that is, a password.

After completing your policy configuration using the Policy Wizard, you can enter and manage users from the **User Files** panel under the **File Tools** folder on the Navigation pane.

Database

Use the Database option if you store or plan to store user profiles in a SQL database. 8950 AAA provides support for most SQL servers. By default the PolicyAssistant uses the built-in 8950 AAA database. However, it is possible to use the PolicyAssistant with most external databases. For support of all other databases, contact the 8950 AAA technical support team.

Use the **User Profiles** panel under the **Database Tools** folder to manage the user profiles stored in the built-in 8950 AAA database.

> **Important!** If you do not see the Database Tools folder on the Navigation pane, select **Preferences** from the Edit menu. Select the **Database** option from the Server Management Tool panel, and click **Display the Database panels in the Navigation pane**.

LDAP Directory

If you are using an LDAP directory as a user profile source, then the authentication source must be either the LDAP server, an ACE/Server, or a SafeWord server.

> **Important!** Use this option if users are stored in an LDAP directory as inet orgPersons, as defined in RFC 2798.

Microsoft Active Directory

Microsoft Active Directory should only be used as a user source when 8950 AAA is not running on a Windows platform.

Windows Security Access Manager

The Windows Security Access Manager (SAM) system option is only available when 8950 AAA is running on a Windows platform. This option should be used instead of Microsoft Active Directory via LDAP when using a Windows platform with access to necessary domain controllers.

UNIX System

The UNIX system option is only available when 8950 AAA is running on a supported UNIX/Linux platform.

UNIX Password File

Use the Password File option if this policy will use standard UNIX password/shadow files pas its user source *(/etc/passwd or /etc/shadow)*.

Your password or shadow files must be formatted in standard UNIX password file format (for a full description, see the UNIX password man page, section 4 or 5). The 8950 AAA server requires you to place the user's name in column one in the file. Passwords, if included, may be encrypted with DES, MD5, or SHA1.

RSA ACE/Server (SecurID)

RSA Ace/Server (SecurID) is not presently available when 8950 AAA is running on Macintosh OS X.

Secure Computing SafeWord Server

If using a Secure Computing SafeWord Server as a user profile source, then the authentication source must be the same server.

Radius Server (Proxy)

Use the RADIUS Server Proxy option if your users are stored in a remote server. Proxy services allow a RADIUS server to forward a request received from a client to a second RADIUS server. Since the RADIUS server is acting on behalf of the client 8950 AAA uses the term "proxy." The RADIUS request is sent to the remote RADIUS server and the response is used to determine the information that is sent to the client.

Important! If you selected ACE/Server, Safe Word, or Proxy as your user profile source, you will not see the Authentication Source Panel. These servers perform authentication and authorization, and notify the 8950 AAA server whether the request is accepted or declined.

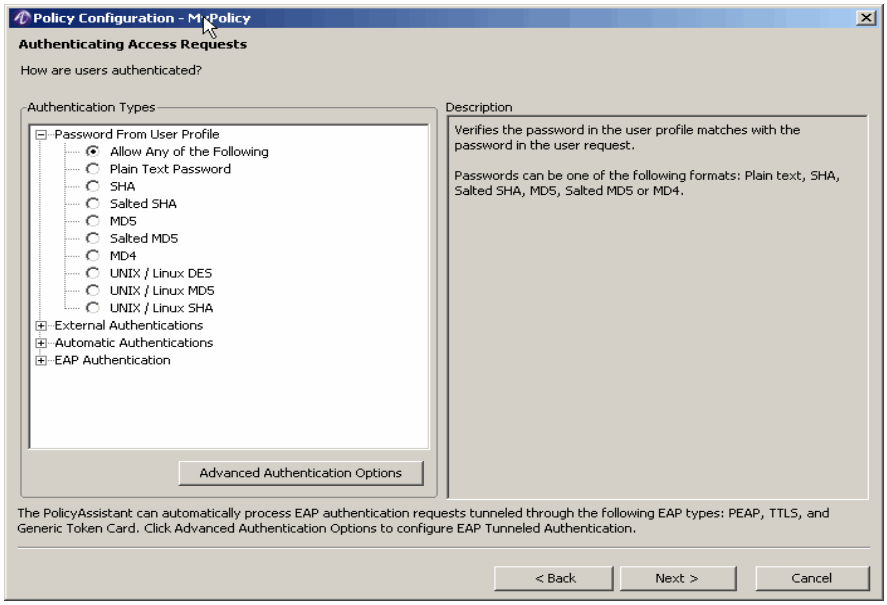
Important! If you are using ACE/Server, Safe Word, or Proxy as your profile source, go to the section *"Defining Accounting Activities" on page 13*.

None

Specifies that the user profiles will not be read. This is typically used in tunnel authentication when EAP Identity is not contained in the outer layer.

Select your user profile source by clicking on the required radio button, and click **Next**. The **Authentication Access Requests** panel appears as shown in Figure 9-5.

Figure 9-5 Authentication Access Requests Panel in the Policy Wizard



To determine a method for authenticating users, select an **Authentication Type** from the list that appears within the Authentication Types pane, as shown in Figure 9-5. This pane contains four categories of Authentication Types as follows:

- Password from User profile
- External Authentications
- Automatic Authentications
- EAP Authentication

The actual options available in this panel are dependent on the choice you made for your user profile source. Table 9-1 lists the options with descriptions.

Table 9-1 Authentication Types

Option	Description
Password from User profile	Select an option from this section if this policy uses text passwords stored in the user profile
Allow any of the following	Verifies the password in the user profile matches with the passwords in the user request. Passwords can be any of the following formats: Plain text, Secure Hash Algorithm (SHA), salted SHA, Message Digest 5 (MD5), Salted MD5, or Message Digest 4 (MD4)

Table 9-1 Authentication Types

Option	Description
Plain Text Password	Verifies the password in the user profile matches with the passwords in the user request. Passwords must be in plain text format.
SHA	Verifies the password in the user profile matches with the passwords in the user request. Passwords must be in SHA format.
Salted SHA	Verifies the password in the user profile matches with the passwords in the user request. Passwords must be in Salted SHA format.
MD5	Verifies the password in the user profile matches with the passwords in the user request. Passwords must be in MD5 format.
Salted MD5	Verifies the password in the user profile matches with the passwords in the user request. Passwords must be in Salted MD5 format.
MD4	Verifies the password in the user profile matches with the passwords in the user request. Passwords must be in MD4 format.
UNIX/Linux DES	Verifies the password in the user profile matches with the password in the user request. Passwords in the profile must be UNIX/Linux DES format.
UNIX/Linux MD5	Verifies the password in the user profile matches with the password in the user request. Passwords in the profile must be UNIX/Linux MD5 format.
UNIX/Linux SHA	Verifies the password in the user profile matches with the password in the user request. Passwords in the profile must be UNIX/Linux SHA format.
External Authentications	Select an option from this section if the user password is stored separately from the user profile or if this policy uses an external service for authentication.

Table 9-1 Authentication Types

Option	Description
Windows Security Access Manager	Uses Windows NT or Security Access Manager (SAM) to verify the password in the user request. This option is only supported on Microsoft Windows platforms.
UNIX System	Uses UNIX system functions to verify the password in the user request. This option is only supported on a UNIX platform.
UNIX Password File	Reads the password in the user's entry directly from a UNIX password or shadow file. The password read from the file is used to authenticate the request in place of any password that is in the user profile. The UNIX/Linux password can be one of the following formats: UNIX Crypt, MD5, SHA, or SSHA. Although primarily used on UNIX platforms, this option can be used to read users from a UNIX password style file on any platform.
RSA ACE/Server (SecurID)	Uses an RSA Ace Server to verify the one time password from a SecurID token.
Secure Computing SafeWord Server	Uses the SafeWord Server from Secure Computing to verify the one time password.
LDAP Directory	Connects to an LDAP Server using the User-Name and password from the request. If the LDAP connection is successful, the user is authenticated.
Microsoft Active Directory	Connects to a Microsoft Active Directory Server using the User-Name and password from the request. If the Active Directory connection is successful, the user is authenticated.
Automatic Authentications	These options skip the password check and either automatically accept or reject all users.
Accept All Request	The password is not checked. However, other checks defined in this policy, including session limits, are still enforced.

Table 9-1 Authentication Types

Option	Description
Reject All Request	Automatically rejects the request. Typically used to disable access for a Policy.
EAP Authentication	EAP Authentications are typically used in conjunction with the Ethernet 802.1x standard. Typical applications are Wi-Fi networks and smart Ethernet switches. Use of EAP requires support from the client supplicant software and access point. For more information contact your client software or access point vendor.
EAP MD5 EAP TLS EAP LEAP EAP LEAP (NT password) EAP LEAP (Plain text password) EAP LEAP (MD4 password) EAP MS CHAP V2 EAP MS CHAP V2 (NT password) EAP MS CHAP V2 (Plain text password) EAP MS CHAP V2 (MD4 password)	Use of EAP requires support from the client supplicant software and access point. For more information contact your client software or access point vendor.

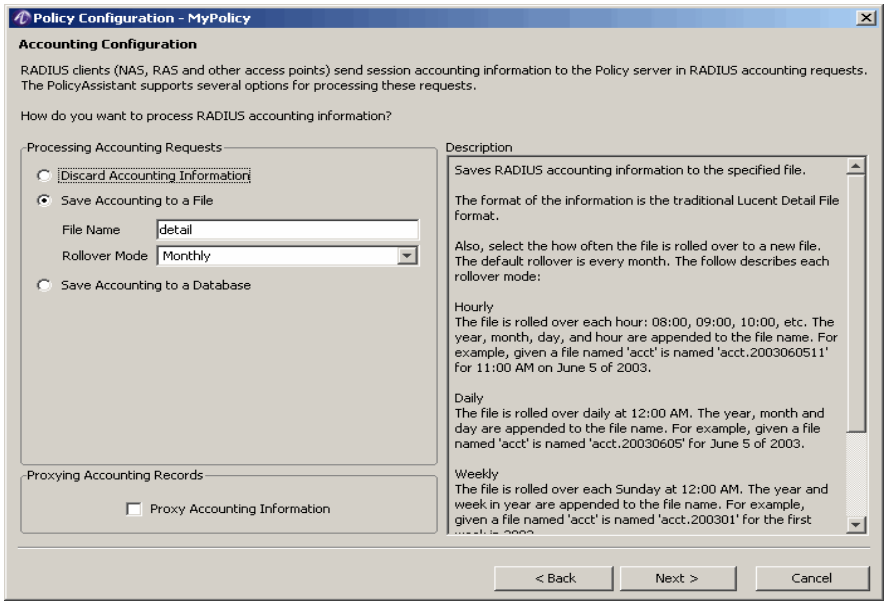
Click the icon that precedes each category to display the list of types. To use one of the types, click its associated button. The types are described within the right pane of the window.

Click **Advanced Authentication Options** to configure additional authentication options. See "Advanced Authentication Options" on page 30, at the end of this chapter.

Click **Next** to configure accounting activities. The Accounting Configuration panel appears as shown in Figure 9-6.

Defining Accounting Activities

Figure 9-6 Accounting Configuration Panel in the Policy Wizard



The accounting configuration step is used to determine how accounting data is processed. 8950 AAA allows this policy to save accounting data to a RADIUS Detail file (specially formatted text file), an SQL database. This policy may also proxy data to another server. The upper left pane of the panel, as shown in Figure 9-6, shows three methods for processing accounting data as follows:

- Discard Accounting Information
- Save Accounting Information to a File
- Save Accounting in a Database

Beneath this pane, is an additional option that allows accounting information to be proxied to another server. The panel describes each selection within the right pane. If you choose to send accounting data to a database or proxy server, the Policy Wizard helps you configure 8950 AAA at a later point.

If you choose **Discard Accounting Information**, then accounting data will not be saved.

If you choose to save your accounting data to a file, enter the **File Name**. 8950 AAA creates the file when accounting activity is initiated by a RADIUS request. 8950 AAA saves and stores the file in the *\run\radacct* directory with the file name you entered and appends a date/time format depending on the rollover mode you select. Select a **Rollover Mode** that defines at which intervals the server will create a new accounting file.

The Description frame on the right of the panel describes the different modes. For example, for the policy configuration, the server creates a file with the name *mydetail2010052708* indicating the file was created at 8:00 AM on May 27, 2010.

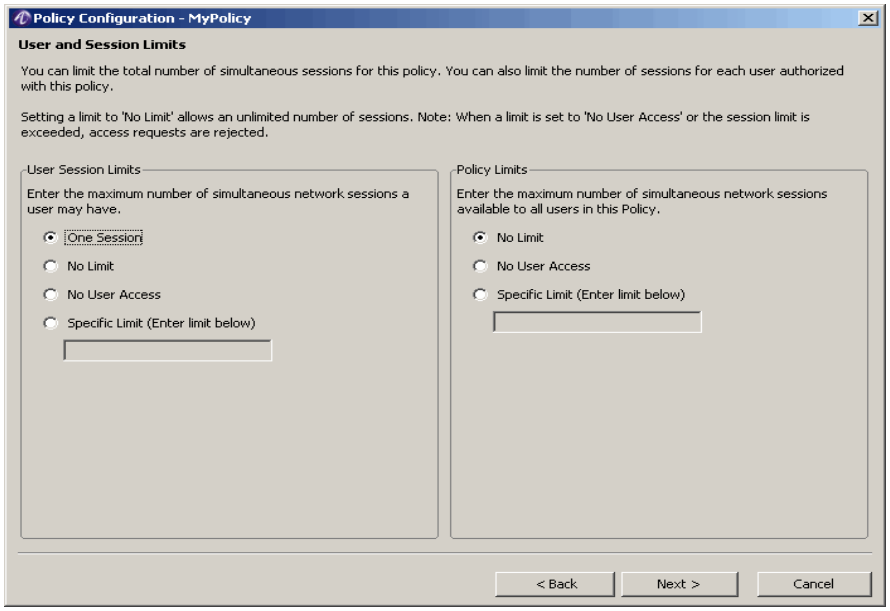
By default, if you choose to save accounting data to an SQL database, the PolicyAssistant uses the built-in 8950 AAA database. Accounting records can be managed by using the Database Tools panel.

If you want to forward your accounting data to a remote server, select **Proxy Accounting Information**. This option is available regardless of the processing option you choose in the top frame of this panel.

Click **Next** to set user and session limits. The User and Session Limits panel appears as shown in Figure 9-7.

Defining Policy Limits

Figure 9-7 User Session and Policy Limits Panel in the Policy Wizard



The *User Session Limits* setting sets the maximum number of concurrent sessions that a user may have. The *Policy Limits* setting indicates the maximum number of concurrent sessions that may be open among all users whose access was controlled by this policy.

The 8950 AAA server checks user session and policy limits independently. If either limit is exceeded 8950 AAA rejects the access request.

For example, assume there is policy for all users at the realm “myisp.com” and in that policy **User Session Limits** is set to 1 and Policy Limits is set to 3.

The users user1@myisp.com, user2@myisp.com, and user3@myisp.com all log in to the network. At this point, the session count for each is 1, so any attempt by these users to log in and start another session, would be rejected. The session count for the policy, is 3. If

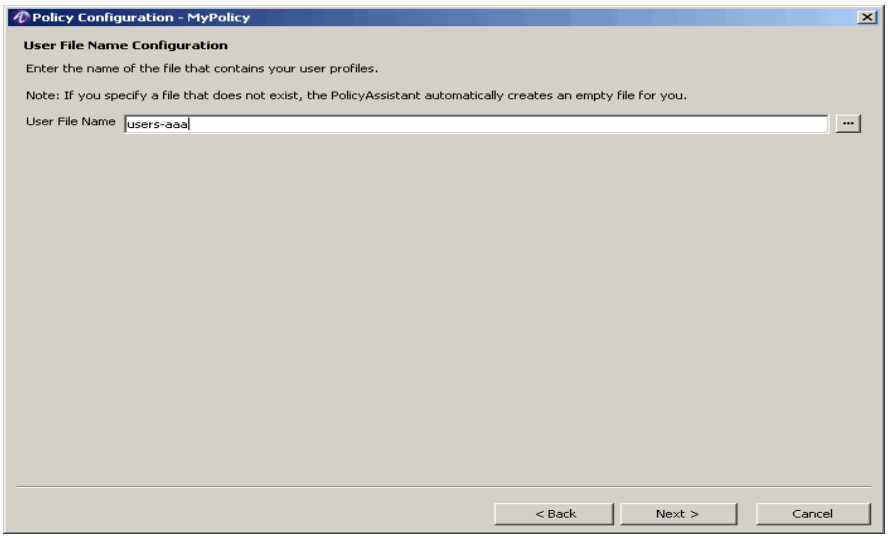
another user, for example, user4@myisp.com, now attempts to log on the 8950 AAA server rejects the access request. In this case, user4's session would exceed the Policy limit, even though the session would not have exceeded the User Session Limit.

When you click **Next**, the Policy Wizard displays panels necessary to configure the user profile, authentication, and accounting choices that you have made in the previous Policy Wizard panels. The number and types of panels that appear are dependent on the options you selected. These panels are documented at the end of this chapter. After completing these panels, the Policy Wizard will display the **Attributes Set for Policy** panel. This configuration option of the Policy Wizard enables you to assign attribute sets to your policy. The following section introduces attribute sets and provides the instructions necessary to complete a policy configuration.

Click **Next** to set the user file name configuration. The User File Name Configuration panel appears as shown in Figure 9-8.

Setting the User File name Configuration

Figure 9-8 User File Name Configuration Panel in the Policy Wizard



Enter the name of the file that contains your user profiles.

Click **Next** to set the Attribute Set for the Policy. The User File Name Configuration panel appears as shown in Click **Next** to set the user file name configuration. The User File Name Configuration panel appears as shown in Figure 9-8.

Understanding and Creating Attribute Sets

About Attribute Set

8950 AAA uses two key actions during Access-Request processing to authorize users and configure user sessions upon successful authentications: performing *authorization checks* and *session provisioning*. Attributes contain the information used to support these actions. Other RADIUS servers generally require that you set this type of information as part of each user's profile. With the PolicyAssistant it is possible to create an *attribute set* for a policy which contains the information that the server applies to all users of the policy.

Authorization checks are logical tests of information that accompany a user's access request or that are known about the request (for example, the date and time a request is received) against a set of authorization rules. The server tests the information it receives against verification attributes, also called *check-items*, stored in an *attribute set* or possibly a user's profile. By including appropriate verification attributes in a policy, a variety of rules can be enforced. For example, users might be permitted to use ISDN connections, required to dial-in to a particular phone number, or use a specific access protocol, such as PPP. Table 9-9 lists attributes commonly used as verification attributes.

Figure 9-9 Sample List of Verification Attributes

Attribute Name	Description of Use of this Attribute as a Verification Attribute	Example
NAS-IP-Address	Limits access to requests sent from a NAS at this IP Address	**NAS-IP-Address = 10.0.1.2**
Service-Type	Only allow requests of this service type	**Service-Type = Framed-Protocol**
Framed-Protocol	Only allows requests that only use the specified Framed-Protocol	**Framed-Protocol = PPP**
Called-Station-Id	Limits access to sessions that were made through this phone number.	**Called-Station-Id = 5105551212**
NAS-Port-Type	Only accept this type of connection. (i.e., ISDN or Async—Analog).	**NAS-Port-Type = Async**
Expiration	Rejects Access-Requests placed after the specified date.	**Expiration = "Mar 27 2005"**
Activation	Rejects Access-Requests placed before the specified date.	**Activation = "Dec 25 2005"**

Figure 9-9 Sample List of Verification Attributes

Attribute Name	Description of Use of this Attribute as a Verification Attribute	Example
Time-Of-Day	Define allowed access times by day-of-week and/or hour-of-day.	**`Time-Of-Day = Wk0800-1700`**

The 8950 AAA server supports session provisioning by returning reply attributes to the NAS upon a successful authentication. Reply attributes, stored in a attribute set, or possibly a user profile, provide additional parameters the NAS needs to complete an access request. By including appropriate reply attributes in a policy, a variety of connection configurations can be applied. For example, a user can be assigned a specific IP addresses, IP header compression can be turned on or off, or a time limit can be assigned to the connection. Table 9-2 lists attributes allowed in an Access-Accept that are commonly used as reply attributes.

Table 9-2 List of Attributes allowed in an Access-Accept available as Reply Attributes

Attribute Name	Description	Required	Max
User-Name	Sets the User-Name for the session. Use if the NAS should send accounting for a name other than the name used for authentication	No	1
Service-Type	The type of protocol. Typically set to “Framed-Protocol” for IP networks.	No	1
Framed-Protocol	The framing protocol to be used, typically PPP.	No	1
Framed-IP-Address	Assigns an IP Address for the session	No	1
Framed-IP-Netmask	Assigns a Netmask for the session	No	1
Filter-Id	Sets an IP filter to use for the session. The filter must have been defined or be available to the NAS.	No	No limit

Table 9-2 List of Attributes allowed in an Access-Accept available as Reply Attributes

Attribute Name	Description	Required	Max
Reply-Message	Sends a message back to the NAS to be displayed to the user. In Windows networking this message may be logged but is not directly displayed to the user.	No	No limit
Vendor-Specific	Used for encoding proprietary vendor specific attribute (VSA) extensions to the RADIUS protocol. See your NAS vendor's documentation for a list of VSAs they support.	No	No limit
Session-Timeout	The maximum allowed session length (in seconds)	No	1
Idle-Timeout	The maximum idle time allowed for the session.	No	1
Port-Limit	The total number of sessions that can be linked together for creating greater bandwidth (Typically used with ISDN sessions.)	No	1

If a reply attribute differs from the nature of the user's session, the NAS must resolve the problem. For example, if the user connects using PPP and 8950 AAA returns a Framed-Protocol attribute set to "SLIP" the NAS should drop the session.

With the 8950 AAA PolicyAssistant it is possible to define attribute sets that apply to all users of a policy. This means that individual user profiles need only contain a user name and password. All other attributes for authorization checks and provisioning rules can be contained in an attribute set for the policy. This makes system management much easier for the administrator.

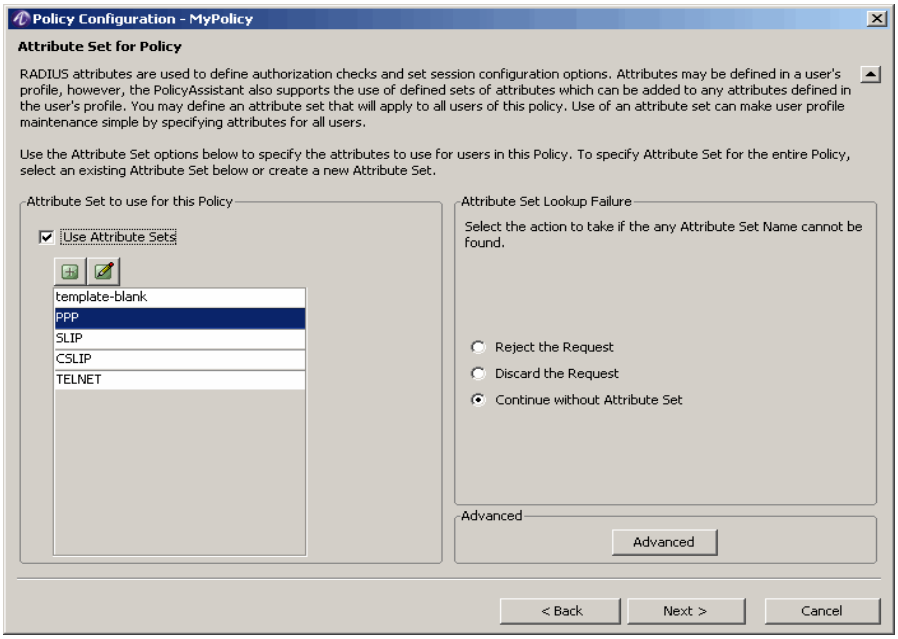
Changing authorization checks and session provisioning can be accomplished by editing the attribute set. This eliminates the need to edit numerous user profiles each time policy changes.

Adding Attribute Sets to Your Policy

About adding Attribute sets

This section covers the use of the Policy Wizard to create attribute sets and assumes that you are creating or editing a policy and have already completed the following configuration steps: defining a user profile source, defining an authentication source, defining storage for accounting data, and setting session limits. You should now see the Attribute Set for Policy panel as shown in Figure 9-10.

Figure 9-10 Attribute Set Panel in the Policy Wizard



If you do not want to use an attribute set with this policy, make sure the option **Use Attribute Sets** is not selected and click **Next** to advance to the final Policy Wizard panel. Please refer to the section "Reviewing Your Policy" on page 25 to complete the Policy Wizard.

Use Attribute Sets

To use attribute sets with this policy, select **Use Attribute Sets**. This is the default setting.

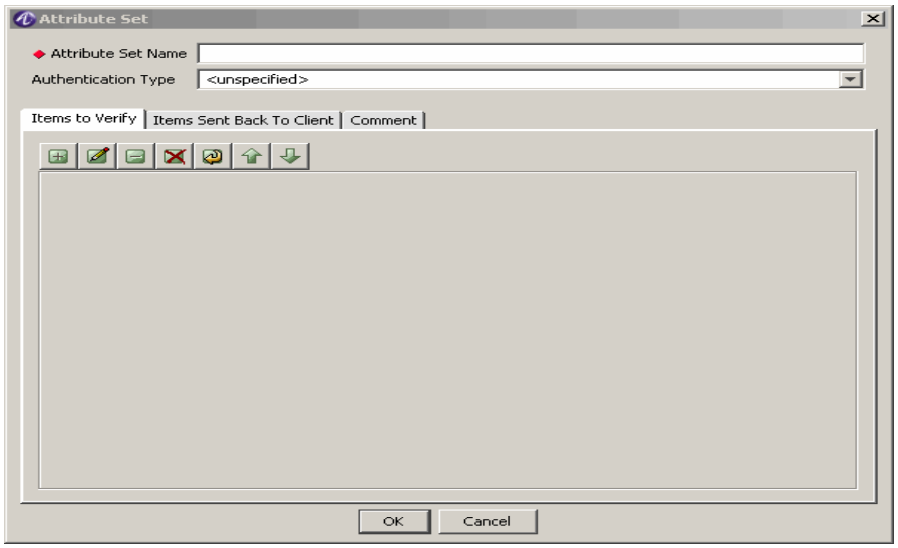
You set which attribute set is used for this policy in the **Attribute to use for this Policy** frame.

Creating Attribute Sets

The following procedure lists the steps to create or edit an Attribute Set:

1. To edit an existing *attribute set*, select its name from the scroll list
   Or
   To define a new set, click **Insert a record** button.
2. The Attribute Sets panel appears as shown below. If you are editing an attribute set the panel will be populated with information about the attribute set you chose.

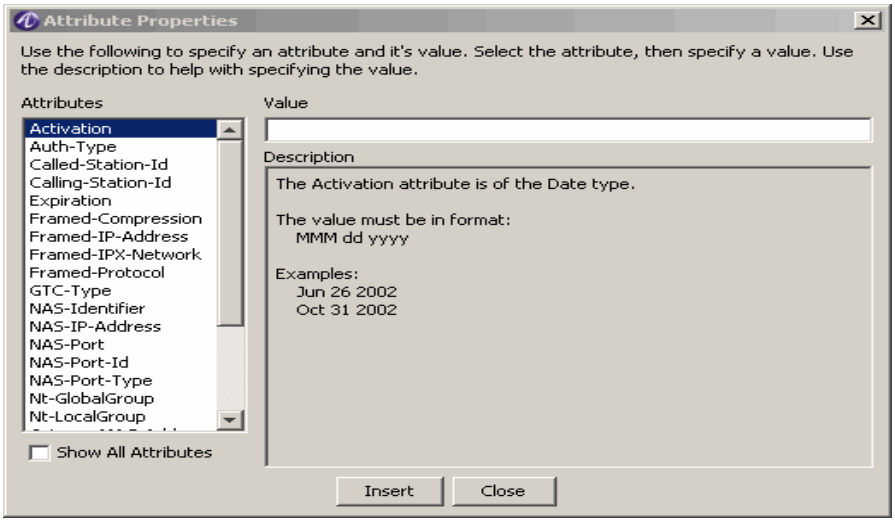
Figure 9-11 Add or Edit Attribute Sets Panel



1. If you are defining a new attribute set, enter a name for this set in the **Attribute Set Name** field.
2. Click the **Items to Verify** tab (by default, this tab is selected when you first enter the Attribute Sets panel) to add or edit verification attributes for this policy.

   You will need to add verification attributes if you want the server to perform authorization checks for this policy.
3. Click **Insert a record** button to open the Attribute Properties panel as shown in Figure 9-12.

Figure 9-12 Attribute Properties Panel



a. Select an attribute from the **Attributes** list and enter or select an appropriate **Value**.

Important! If you also have verification attributes in a user profile, in case of conflicts the attribute setting from the user profile will be applied.

The Description below the Value field, provides guidelines on the format for those attributes that support data input entered from the keyboard.

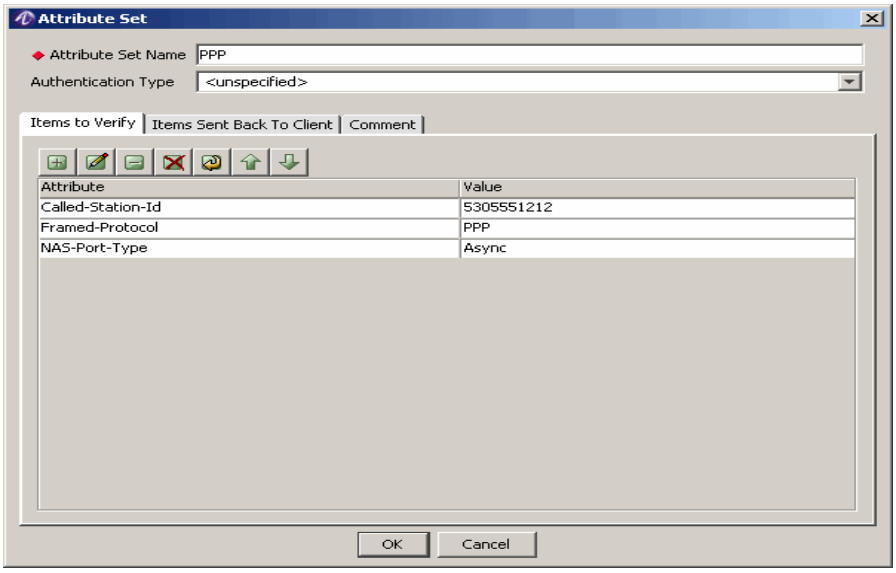
Click **Show All Attributes** to display all attributes included in the server dictionary; otherwise, the list of attributes is limited to those attributes that were defined in the SMT preferences check-items list panel.

Important! To change the attributes that appear in this list, select Preferences from the Edit menu. Select the Check-items List option from the Server Management Tool Preferences panel.

b. Click **Insert** to add the attribute. To insert additional attributes, return to Step a.

c. Click **Close** when you are done adding attributes. The verification attributes you selected are displayed on the Items to Verify tab.

Figure 9-13 Items to Verify Tab of the Attribute Sets Panel



4. Click the **Items Sent Back to NAS** tab to add reply attributes for this policy.

   You need to add reply attributes if you want the NAS to configure the session uniquely for this policy. The server returns these attributes to the NAS if the authentication and authorization steps are successful. This is referred to as *provisioning* the session.

5. Click **Insert a record** to open the Attribute Properties panel.

   a. Select an attribute from the **Attributes** list and enter or select an appropriate **Value**. For example, you can limit the session time to one hour, select the *Session-Timeout* attribute and enter `3600` in the Value field; or identify a specific IP address pool from which addresses are assigned., select the *Ascend-Assign-IP-Pool* attribute and enter an appropriate value in the Value field.

   The Description below the Value field, provides guidelines on the format for those attributes that support arbitrary data entered from the keyboard.

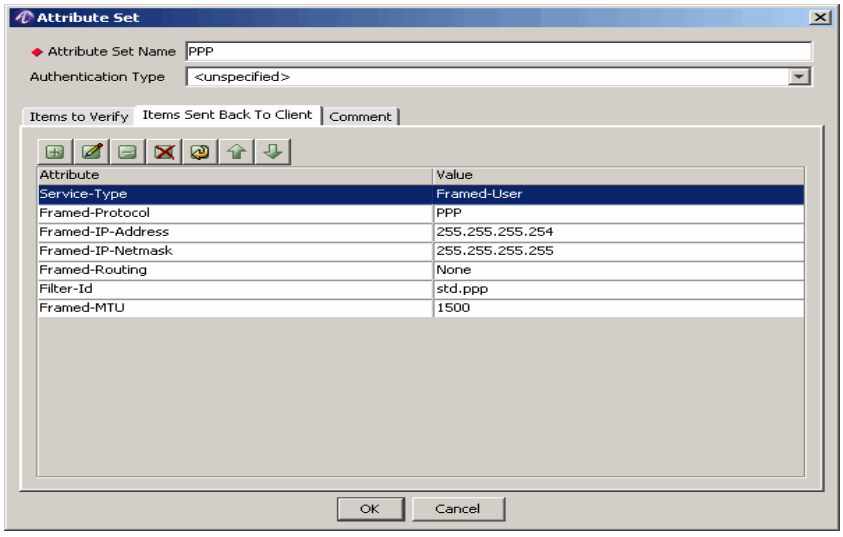
   Click **Show All Attributes** to display all attributes included the dictionary selected in the server profile.

   Important! To change the attributes that appear in this list, select Preferences from the Edit menu. Select the Reply-items List option from the Server Management Tool Preferences panel.

   b. Click **Insert** to enter multiple attributes.

   c. Click **Close** when you are done adding attributes. The reply attributes you configured appear under the **Items Sent Back to NAS** tab.

Figure 9-14 Items Sent Back to NAS tab of the Attribute Sets Panel



6. Click **OK** to close the Attribute Sets panel and return to the Attribute Set for Policy panel in the Policy Wizard. The attribute set you create appears in the scroll list under the Attribute Set Lookup frame. The set is added to the file listed under the Advanced tab.

Defining a Failure Mode

About the Failure Mode

Use the options in the **Attribute Set Lookup Failure** frame to define the action the PolicyAssistant should take in the event an Attribute Set cannot be found. Such a failure might be caused by an error in a Session-Template attribute in a User Profile, or by an error when giving the Attribute Set a name.

The three options, are as described below in Table 9-3.

Table 9-3 Attribute Set Options

Option	Description
Reject the Request	Send an access-reject response to the NAS. The server ends the session immediately.
Discard the Request	Stop processing the request, but do not send any reply to the NAS. The NAS may retry sending the request to another 8950 AAA server, where a copy of the Attribute Set might be available.

Table 9-3 Attribute Set Options

Option	Description
Continue without the Attribute Set	Continue processing the request, but without the attributes from the Attribute Set. If authentication and authorization are successful the Access-Request is sent. However, the session may not function as intended or may not start at all. This is the default setting.

Setting the Location for Your Attribute Sets

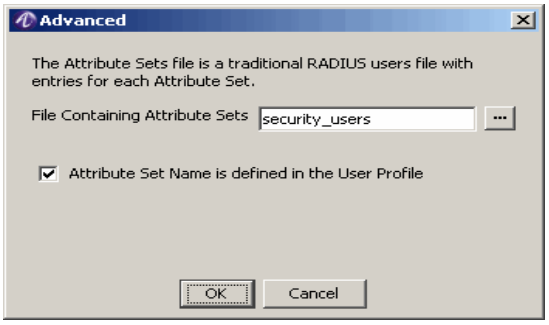
If you choose to define an attribute set for an individual in addition to the set assigned to all users of this policy, you must store all sets in the same file. The PolicyAssistant includes a template file (*\run\users.template*) that stores the predefined attribute sets. It is recommended to add your unique attribute sets to this file.

1. Click **Advanced** to open the Advanced panel.
2. Enter a name in the **File Containing Attribute Sets** field. The file must already exist and be located in the 8950 AAA *run* directory. If the file cannot be found or if the named Attribute Set cannot be located in the file the PolicyAssistant follows the action defined above in the **Attribute Set Lookup Failure** frame.
3. Click **Attribute Set Name is defined in the User Profile** to identify the user profile as a source for your attribute sets.

   Use this option if your user profile source is one of the sources that store only user name and password to create unique attribute sets for any of your users.

   For example, your user profile source is SecurID and the account for user ‘kyle’ will be deactivated at the end of the month. Use the process defined in the section “Creating Attribute Sets” on page 20 to create an attribute set with the name ‘kyle’ that includes the deactivation attribute under the **Items to Verify** tab. Click **Advanced** button. The **Advanced** option is displayed, as shown in Figure 9-15.

Figure 9-15 Policy Configuration-PolicyAssistant Advanced Attribute Sets option



Click on the **...** and a list of files containing the existing Attribute Sets are displayed. Select one of the Attribute Sets and select the **Attribute Set Name is defined in the User Profile** checkbox. Click **OK**. The Attribute Set for Policy panel is displayed as shown in Figure 9-10. Figure 9-10 now displays the values of the Attribute sets from the set that was selected.

When the 8950 AAA server receives a request from user ‘kyle’, it forwards the packet to the SecurID server for authentication. If accepted the packet is returned to the 8950 AAA server, which then looks up the attribute set using the User-Name attribute. If the packet passes the Items to Verify checks, in this case if the deactivation date is not exceeded, the request is authorized and accepted.

4. Click **Next** to complete the Policy Wizard.

Reviewing Your Policy

How to review your policy

This concludes the configuration steps using the wizard.

Click **Next** to view your policy, and click **Finish** to close the wizard.

Using the PolicyAssistant

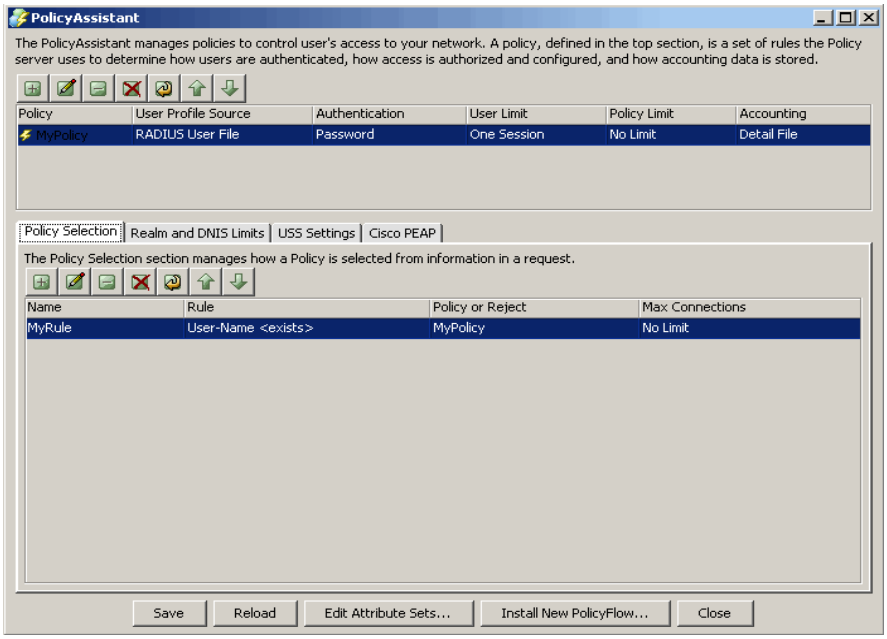
About Using the PolicyAssistant

After creating a policy, you must decide how to route incoming requests to a specific policy. 8950 AAA enables you to use a realm name or a DNIS number to identify the correct policy for your users. For example, you may need to group corporate users by the domain they belong to or the access number they dial when traveling. The Policy Assistant panel, as shown in Figure 9-16, has two sections. The PolicyAssistant section, which is the top section, allows you to create/configure new Policies, manage policies to control user

access to your network. A policy is a set of rules the Policy server uses to determine how users are authenticated, how access is authorized and configured, and how accounting data is stored. The bottom section contains four tabs that allows you to manage a selected policy:

- Policy Selection
- Realm and DNIS Limits
- USS Settings
- Cisco PEAP

Figure 9-16 Policy Assistant Panel



Using the Policy Selection tab

The Policy Selection section allows you to manage a selected policy. A set of action buttons, as shown in the Figure 9-17, appear on the bottom of this section when you select the Policy Selection tab.

Figure 9-17 Policy Selection tab-Action Buttons

The action buttons allow you to perform the following actions:

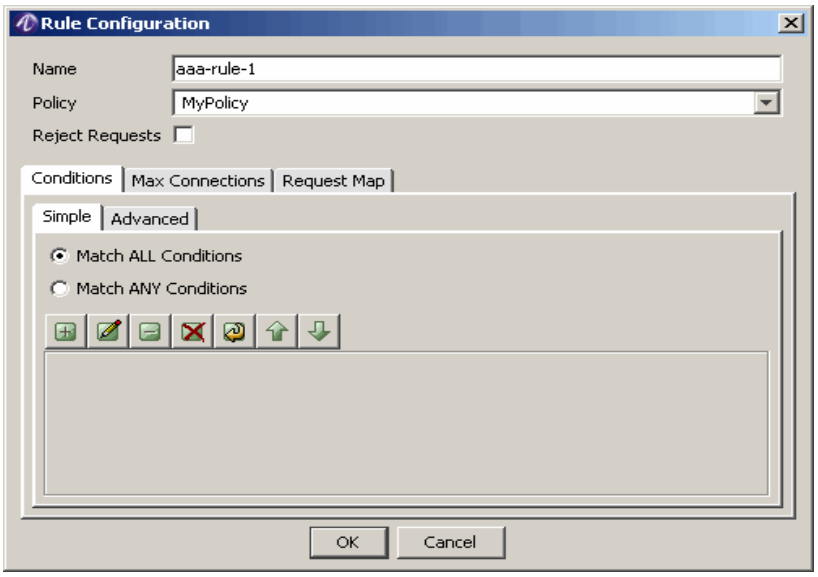
- Insert a record
- Edit a record
- Delete a record

- Delete all records
- Make a copy of selected records
- Move selected record up
- Move selected record down

These action buttons allows you to perform appropriate actions.

1. To add a new Rule configuration, click on the insert a record,  action button. The Rule Configuration panel is displayed as shown in the Figure 9-18. This screen allows you to add policy rule configurations.

Figure 9-18 Policy Assistant-Rule Configuration Panel



2. There are three tabs in the Rule Configuration panel namely, Conditions tab, Max Connections, and Request Map tab. These allow to select an attribute to the Rule and specify the value of it. It also allows you to choose if the rule has to match all the conditions or just match any of the conditions and define the rule. The Rule configuration you added will now be displayed in the main screen, Figure 9-16.
3. The Edit, delete, delete all, copy, move up, move down buttons allows you to perform necessary actions on the defined or existing Rule Configurations.

Defining Realms

Many ISPs use a realm name to identify the home ISP enabling traveling users to access networks of other ISPs when roaming agreements are in place. Use a realm name or any name that distinguishes the type of services provided by the policy. If you plan to route incoming requests using a DNIS, you must create a realm. The following identifies hypothetical group names for the three examples discussed here:

- domain01–for example, *domain01\jsmith*

- tollfree–a name you might use internally to associate the policy with dialed access (DNIS) numbers
- myisp.com–for example, *jsmith@myisp.com*

Defining DNIS

The PolicyAssistant offers a way to associate a DNIS (the RADIUS attribute Called-Station-Id) with a realm. When using DNIS realms all calls to a given DNIS are treated as if the user specified the associated realm, regardless of the realm the user actually entered. This allows use of simple user names without a realm for network connection. If each DNIS is associated with a specific realm, it prevents users of one realm calling a DNIS assigned to another realm (requires that the combination of user name and password is unique for all users).

For example, if the phone number 555-1212 is associated with the realm foo.net and a user eileen@gato.com dials 555-1212 to connect to the network, the 8950 AAA server treats the user as though they were in the foo.net realm ignoring the gato.com realm. The server searches for the user profile in the source defined for the foo.net realm.

If the number (DNIS) dialed by a user is not associated with a realm, then any realm the user entered as part of their User-Name is used as the realm name.

Using the Realm and DNIS Limits tab

The Realm and DNIS tab allows you to manage the number of connections allowed for either a specific Realm or DNIS. You can also limit based on policy and user, which are defined with in the Policy. A set of action buttons, similar to the set shown in Figure 9-17, appear on the bottom of this section when you select the Realm and DNIS tab.

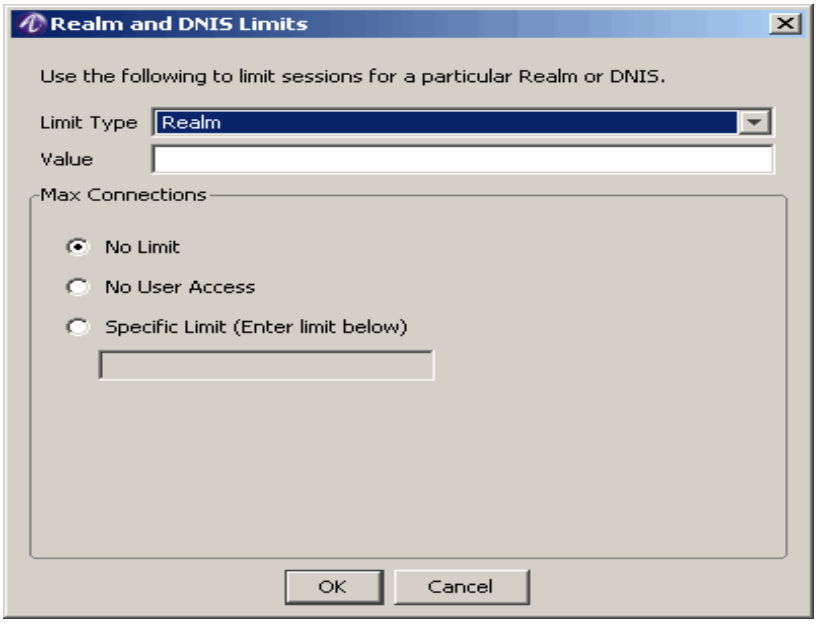
The action buttons allow you to perform the following actions:

- Insert a record
- Edit a record
- Delete a record
- Delete all records
- Make a copy of selected records
- Move selected record up
- Move selected record down

These action buttons allows you to perform appropriate actions.

1. To add a new Realm or DNIS, click on the insert a record, action button. The Realm and DNIS Limits panel is displayed as shown in the Figure 9-19. This screen allows you to limit sessions for a particular Realm or DNIS.

Figure 9-19 Policy Assistant-Realm and DNIS Limits panel



2. Choose the Limit Type as either Realm or DNIS. Provide a value for the Realm or DNIS. Select appropriate Max Connections as either No Limit, No User Access, or Specific Limit. If you choose, Specific Limit, provide the Limit. Click **OK**. The Realm or DNIS value you added will now be displayed in the main screen, Figure 9-16.
3. The Edit, delete, delete all, copy, move up, move down buttons allows you to perform necessary actions on the defined or existing Realm and DNIS Limits.

Using the USS Settings tab

The Universal State Server (USS) settings tab allows you to control the session limits for users, Realms, DNIS, and Policies. You can use this tab to control the USS and where it runs.

When the USS Settings tab is selected, the following list of attributes/values are displayed with appropriate values.

- Use Universal State Server–Yes or No option
- IP Address/Host
- Shared Secret
- Authentication Port
- Accounting Port

Enter or change the values of these fields appropriately and click on **Save** to save the changes.

Using the Cisco PEAP tab

The Cisco PEAP tab allows you to enable Cisco PEAP with the Policy Assistant. If your users are required to be authenticated using PEAP from a Cisco Client, the request does not include realming information.

When the Cisco PEAP tab is selected, the following list of attributes/values are displayed.

- Use Cisco PEAP–Yes or No option
- RSA Certificate File Name
- RSA Private Key Password
- DSA Certificate File Name
- DSA Private Key Password

Enter or change the values of these fields appropriately and click on **Save** to save the changes.

Saving Your Policies

How to save your policies

This concludes the use of the PolicyAssistant to create policies and realms. Click **Save** to store the changes to your policies.

If the 8950 AAA server is running and you have made changes to your policies, Realms or DNIS Limits, USS Settings, and Cisco PEAP, click **Reload** to store your changes and update the active server files.

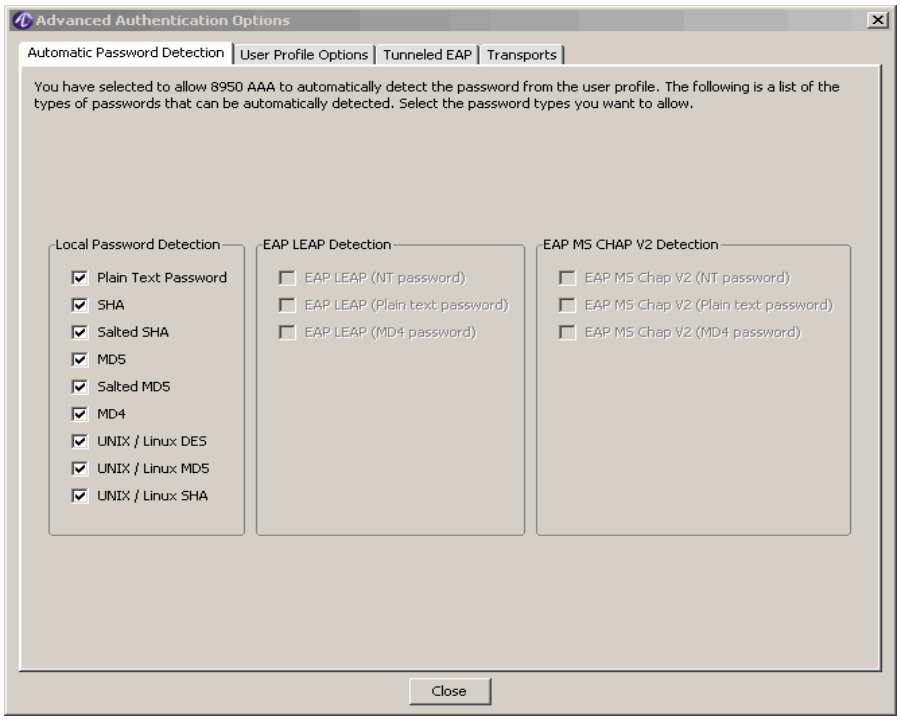
Advanced Authentication Options

About Advanced Authentication options

This section provides additional information for defining authentication source.

The Authenticating Access Requests panel shown in Figure 9-5 on page 9 contains the Advanced Authentication Options button. It provides the ability to fine-tune your definition of authentication source by using the Advanced Authentication Options window, as shown in Figure 9-20.

Figure 9-20 Advanced Authentications Options



The Advanced Authentication Options window contains four tabs:

- **Automatic Password Detection**–Defines the password format types that can be automatically detected by 8950 AAA.
- **User Profile Options**–Defines the options that 8950 AAA can read from the Auth-Type attribute in the user's profile.
- **Tunneled EAP**–Defines tunneled EAP types that the PolicyAssistant can process if EAP tunneling is enabled.
- **Transports**–Defines password transport types that can be used by 8950 AAA.

Table 9-4 lists the options available for each tab.

Table 9-4 Advanced Authentication Option

Tab/Group/Option	Description
Automatic Password Detection	
• Local Password Detection	Automatically detect passwords stored within a user profile
– Plain Text Password	Detect passwords using plain text format
– SHA	Detect passwords using SHA format
– Salted SHA	Detect passwords using Salted SHA format

Table 9-4 Advanced Authentication Option

Tab/Group/Option	Description
– MD5	Detect passwords using MD5 format
– Salted MD5	Detect passwords using Salted MD5 format
– MD4	Detect passwords using MD4 format
– UNIX/Linux DES	Detect passwords using UNIX/Linux DES format
– UNIX/Linux MD5	Detect passwords using UNIX/Linux MD5 format
– UNIX/Linux SHA	Detect passwords using UNIX/Linux SHA format
• EAP LEAP Detection	Automatically detect passwords stored separately from the user profile or using an external service for authentication
– EAP LEAP (NT password)	Detect NT passwords
– EAP LEAP (Plain text password)	Detect plain text passwords
– EAP LEAP (MD4 password)	Detect MD4 passwords
• EAP MS CHAP V2 Detection	Automatically detect passwords stored separately from the user profile or using an external service for authentication
– EAP MS CHAP V2 (NT password)	Detect NT passwords
– EAP MS CHAP V2 (Plain text password)	Detect plain text passwords
– EAP MS CHAP V2 (MD4 password)	Detect MD4 passwords
User Profile Options	
• Password from User File	Use information from user file as specified in Auth-Type attribute
– Plain Text Password	Detect passwords using plain text format
– SHA	Detect passwords using SHA format
– Salted SHA	Detect passwords using Salted SHA format
– MD5	Detect passwords using MD5 format
– Salted MD5	Detect passwords using Salted MD5 format
– MD4	Detect passwords using MD4 format
– UNIX/Linux DES	Detect passwords using UNIX/Linux DES format
– UNIX/Linux MD5	Detect passwords using UNIX/Linux MD5 format

Table 9-4 Advanced Authentication Option

Tab/Group/Option	Description
– UNIX/Linux SHA	Detect passwords using UNIX/Linux SHA format
• External Authentication	Use information from external source as specified in Auth-Type attribute
– LDAP Directory	Detect passwords within LDAP directory
– Microsoft Active Directory	Detect passwords within MS Active Directory
– Windows Security Access Manager	Detect passwords within Windows SAM
– UNIX System	Detect passwords within UNIX System
– UNIX Password File	Detect passwords within UNIX password file
– RSA ACE/Server (SecurID)	Detect passwords within RSA ACE/Server
– Secure Computing SafeWord Server	Detect passwords within Secure Computing SafeWord Server
• EAP Authentication	Use information from EAP source as specified in Auth-Type attribute
– EAP MDS	Detect MDS passwords
– EAP TLS	Detect TLS passwords
– EAP LEAP	Detect all LEAP passwords
– EAP LEAP (NT password)	Detect NT passwords
– EAP LEAP (Plain text password)	Detect plain text passwords
– EAP LEAP (MD4 password)	Detect MD4 passwords
– EAP MS CHAP V2	Detect all MS CHAP V2 passwords
– EAP MS CHAP V2 (NT password)	Detect NT passwords
– EAP MS CHAP V2 (Plain text password)	Detect plain text passwords
– EAP MS CHAP V2 (MD4 password)	Detect MD4 passwords
Tunnelled EAP	
• Available EAP Tunnel Types	Automatically process EAP authentication requests tunneled through tunnel types
– PEAP	Allow PEAP tunnel type
– PEAP with Generic Token Card installed	Allow PEAP with Generic Token Card tunnel type
– TTLS	Allow TTLS tunnel type

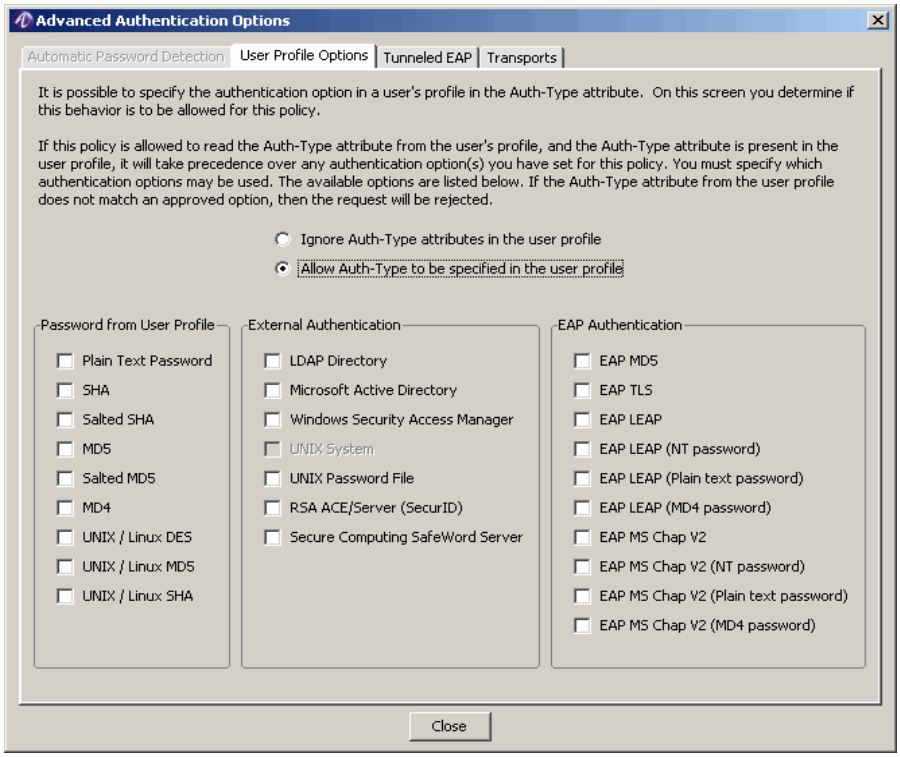
Table 9-4 Advanced Authentication Option

Tab/Group/Option	Description
– TTLS with Generic Token Card installed	Allow TTLS with Generic Token Card tunnel type
– Generic Token Card	Allow Generic Token Card tunnel type
Transports	
• Plain Text Password	Allow Plain Text transport
– Password	Allow Plain Text Password transport
– CHAP-Password	Allow Plain Text Password - CHAP transport
– MS-CHAP-Response	Allow Plain Text Password - MS-CHAP transport
– MS-CHAP2-Response	Allow Plain Text Password - MS-CHAP2 transport
• Salted MD5	
– Password	Allow Salted MD5 transport
• UNIX/Linux DES	
– Password	Allow UNIX/Linux DES transport
• Salted SHA	
– Password	Allow Salted SHA transport
• MD5	
– Password	Allow MD5 transport
• UNIX/Linux SHA	
– Password	Allow UNIX/Linux SHA transport
• MD4	
– Password	Allow MD4 transport
– MS-CHAP-Response	Allow MS-CHAP transport
– MS-CHAP2-Response	Allow MS-CHAP2 transport
• SHA	
– Password	Allow SHA transport
• UNIX/LINUX MD5	
– Password	Allow UNIX/Linux MD5 transport

On the Authenticating Access Requests panel (Figure 9-5), if you selected the option **Allow Any of the Following**, then, after clicking **Advanced Authentication Options**, the Advanced Authentication Options window appears as shown in Figure 9-20. You may customize the list of verified format types by deselecting any check box that corresponds to a undesirable format type.

On the Authenticating Access Requests panel, if you selected any option other than **Allow Any of the Following**, then, after clicking **Advanced Authentication Options**, the Advanced Authentication Options window appears as shown in Figure 9-5.

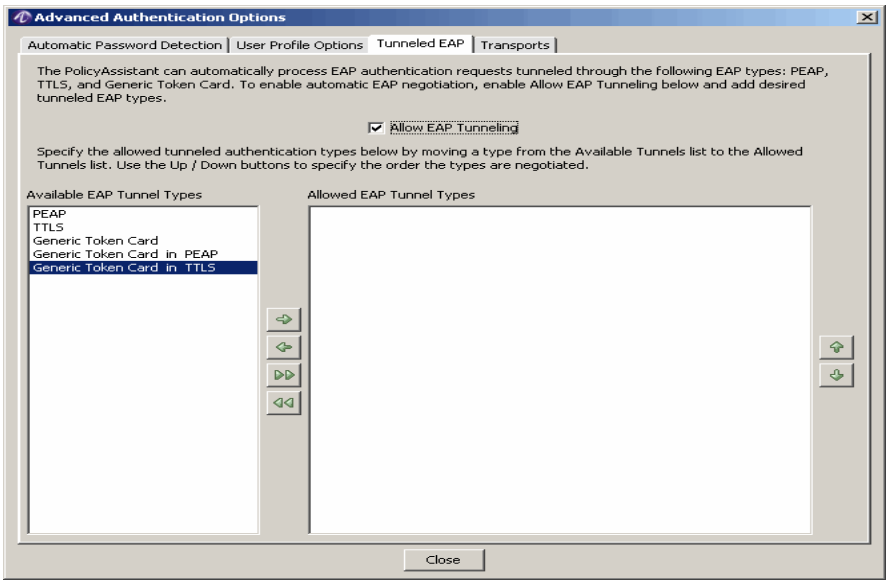
Table 9-5 Advanced Authentications Options-User Profile Options



Tunneled EAP tab option

Click on the Tunneled EAP tab and the following panel is displayed, as shown in Figure 9-21. By selecting the **Allow EAP Tunnelling** checkbox, you can enable automatic EAP negotiation and add desired tunneled EAP types.

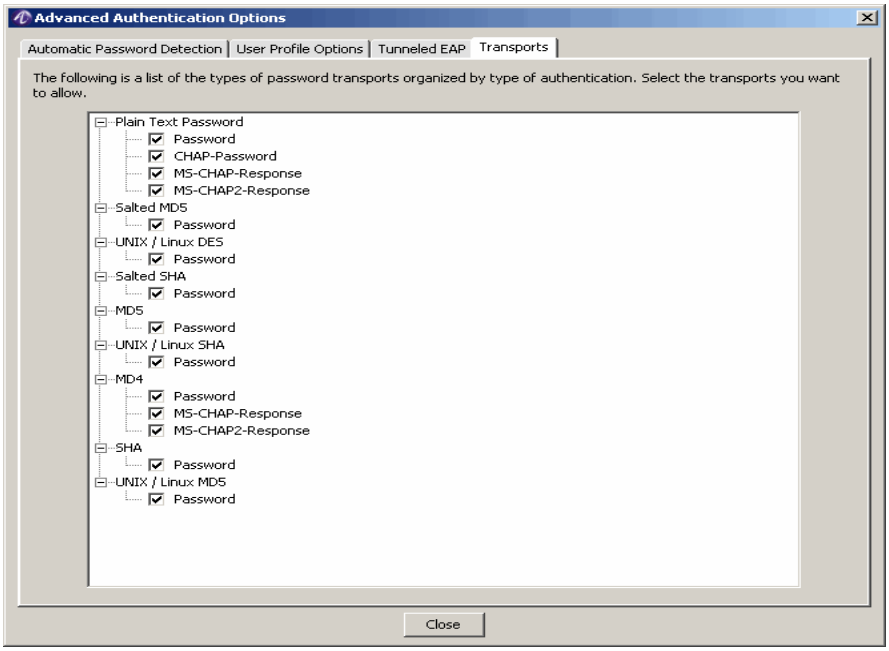
Figure 9-21 Advanced Authentications Options-Tunneled EAP tab Options



Transports tab option

Click on the **Transports** tab and the following panel is displayed, as shown in Figure 9-22. This displays a list of the types of password transports organized by type of authentication. Select the transports you want to allow.

Figure 9-22 Advanced Authentications Options-Transports tab Options



Advanced Attribute Set Options

About Advanced Attribute Set Options

Attribute sets can be referenced from many of the supported user profile sources such as RADIUS user files, database records and LDAP configurations, SecurID ACE Server, UNIX password file or NIS/NIS+ and as part of a policy. This section covers attribute sets defined as part of the policy. Additional information on referencing other templates is provided below.

You may allow an attribute set name to be specified in the users profile. By default this option is enabled, to disable the Attribute Set name from being read from the user profile Attribute Sets, click in the Attribute Name is defined in the User Profile box. In most cases you will probably wish to disable this option.

If this option is enabled, the PolicyAssistant looks for the Session-Template attribute in the Reply Attributes section of the User Profile. If found, the PolicyAssistant attempts to load the named set from the file designated in the Advanced options panel.

It is possible for 8950 AAA to read multiple attribute sets during the processing of a single user request. This might be the case if there was an Attribute Set defined in the User Profile and another set defined for the policy. In this case, the Attribute Set defined in the

User Profile is read first, then the policy set is read. If an attribute is defined in both Attribute Sets, the first assignment read takes precedence. That is, the attribute definition from the User Profile would be the one used in the Access-Accept response.

END OF STEPS

10 Configuring 8950 AAA USSv2

Overview

Purpose

This chapter discusses the process of configuring the 8950 AAA USSv2 functionality.

The following topics are included in this chapter:

USSv2 Configuration

The Universal State Server (USS) and Universal State Server version 2 (USSv2)

The Universal State Server (USS) is an in-memory database optimized to track network-resource usage. It interacts with the 8950 AAA Server to maintain usage counts and enforce resource limits within the network.

The Universal State Server version 2 (USSv2) Configuration feature is an advanced feature of the USS feature. The USSv2 is a brand new design and in many ways different from the USS feature though the basic concepts are same. The new USSv2 is not built on the old USS.

The USSv2 differs from the old USS as following:

- USSv2 is a replication and persistence handling framework that allows “pluggable” state machines.
- USSv2 can handle any number of instances of state machines of the same or different types, each with its own database and set of replication hosts.
- USSv2 replicates in active-active mode and all hosts in a replication domain can service requests at any time.

Using the SMT to configure USSv2

The USSv2 uses in-memory databases to track network resources. The information tracked includes the current state of a network resource and any information associated with that resource about how it is being used. The information associated with the resource can be counted to gather over all network resource usage. The information in the USSv2 can be used to make decisions in the PolicyFlow on how to process the AAA request.

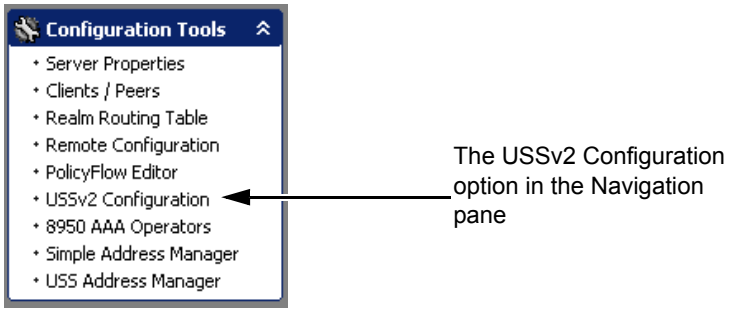
Use the StateServer section below to configure the types of resources you want to track. Use the Replicated Server section to automatically serve a copy of the resource data in other servers (only available with a license enabled for replication).

This section describes how to configure the 8950 AAA USSv2.

For information about running the SMT, please refer to "Starting the Server Management Tool" .

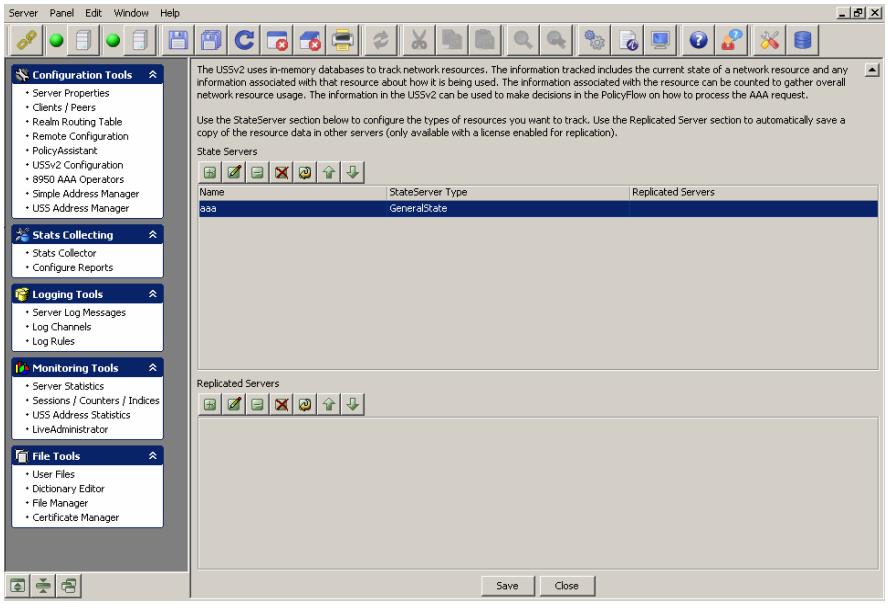
1. Select **USSv2 Configuration** from the Configuration Tools folder on the Navigation pane, as shown in Figure 10-1.

Figure 10-1 Navigation Pane-USSv2 Configuration option



Result: The **8950 AAA USSv2 Configuration** panel is displayed as shown in Figure 10-2.

Figure 10-2 The 8950 AAA SMT-USSv2 Configuration panel



Action buttons of the USSv2 State Servers Section

The **USSv2 Configuration** panel (Figure 10-2) contains two sections that consists of 2 sets of Action buttons that appear in the 8950 AAA USSv2 Configuration panel, as shown in Figure 10-2.

The action buttons that are in the top section are used to configure State Servers. The action buttons that are in the bottom section are used to configure the Replicated servers.

The Top set of action buttons are as shown in Figure 10-3.

Figure 10-3 USSv2 Configuration-Action buttons in the State Servers section

These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

To Insert a record, click on the  action button. The **StateServer Configuration** panel is displayed as shown in Figure 10-4. This panel allows you to add a StateServer and its type as shown in Figure 10-4.

Figure 10-4 The USSv2 StateServer Configuration-Add panel

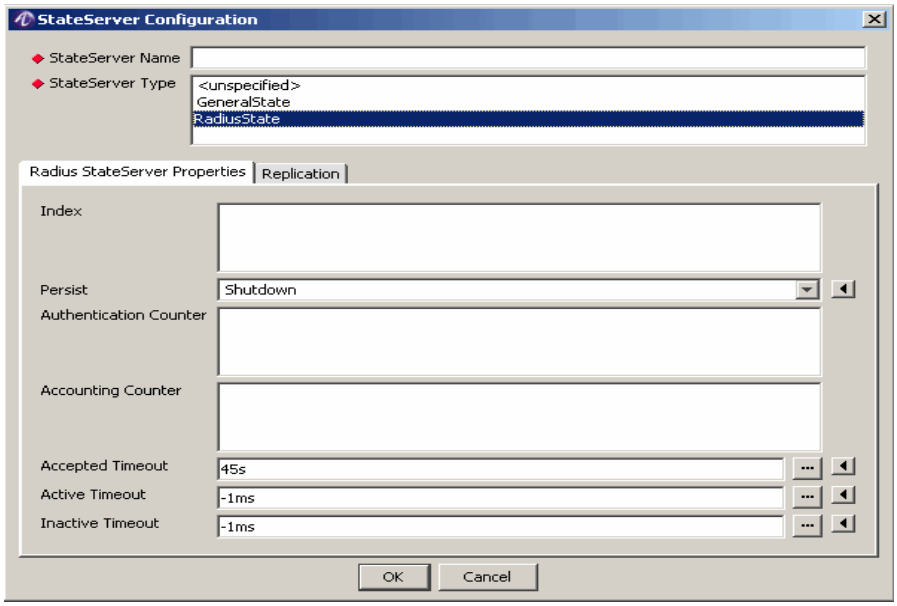


Table 10-1 explains each of these fields and the field descriptions that you need to specify in this screen.

Table 10-1 USSv2 StateServer Configuration Properties

Field Name	Description
StateServer Name	Specifies a unique name for this entry.
StateServer Type	Sets the type of this model from one of the available model types in the system.

The **StateServer Configuration** panel, Figure 10-4, has two tabs: the Properties tab and the Replication tab. The **Properties** tab displays the properties of the StateServer Type that you decide to select. For example, if you select the RadiusState as StateServer Type, the Properties tab will display the Radius StateServer Properties as shown in Figure 10-4.

The other tab, the Replication tab, when clicked will display the Replicated Server properties as shown in Figure 10-5.

Figure 10-5 The USSv2 StateServer Configuration-Replication tab properties

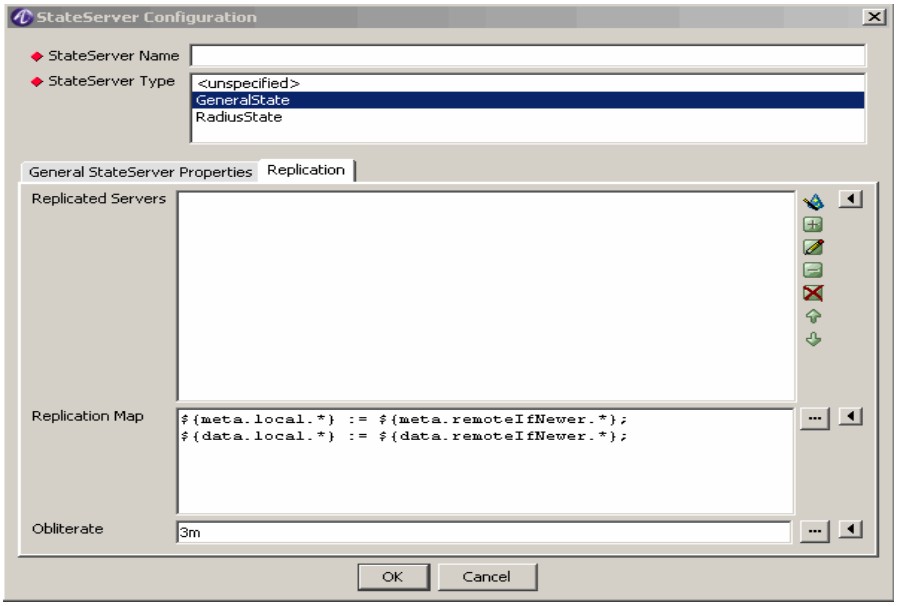


Table 10-2 explains each of these fields and the field descriptions that are displayed in this screen.

Table 10-2 USSv2 StateServer Configuration-Replication tab properties

Field Name	Description
Replicated Servers	A list of zero or more names of defined nodes to which this model will replicate. Note that if any names are given, exactly one of them has to match the name of the local Diameter Origin-Host property of each node.
Replication Map	Specifies the mapping to be applied when merging remotely replicated entries into local, pre-existing entries.
Obliterate	The fall back time-out to use to terminally remove entries marked for deletion out of the database in case a delete event is not acknowledged.

Action buttons of the USSv2 Replicated Servers Section

The **USSv2 Configuration** panel (Figure 10-2) contains two sections that consists of 2 sets of Action buttons that appear in the 8950 AAA USSv2 Configuration panel, as shown in Figure 10-2.

The action buttons that are in the bottom section are used to configure Replicated Servers. The Top set of action buttons are as shown in Figure 10-3 and are as explained earlier.

Figure 10-6 USSv2 Configuration-Action buttons in the Replicated Servers section

These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

To Insert a record, click on the  action button. The **Replicated Server Configuration** panel is displayed as shown in Figure 10-7. This panel allows you to add a Replicated Server and its properties as shown in Figure 10-7.

Figure 10-7 The USSv2 Replicated Server Configuration panel

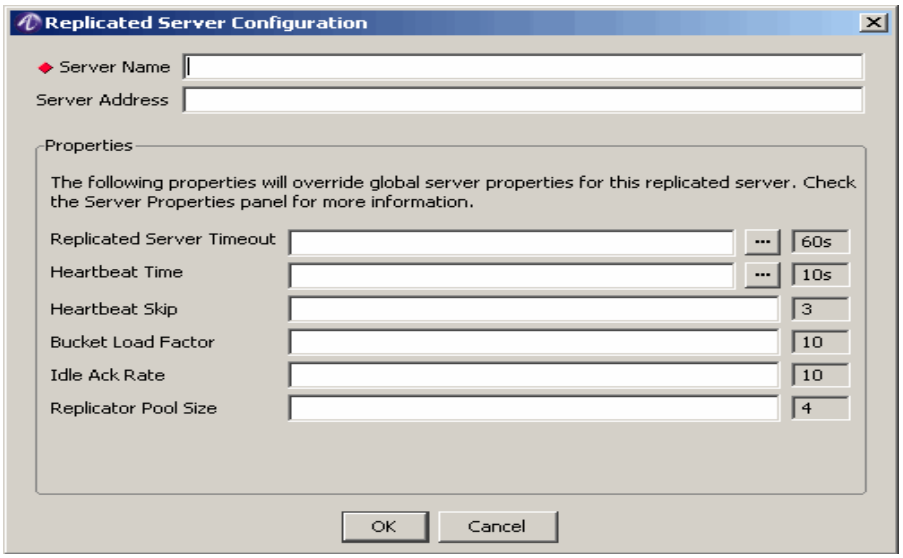


Table 10-3 explains each of these fields and the field descriptions that you need to specify in this screen.

Table 10-3 USSv2 Replicated Server Configuration Properties

Field Name	Description
Server Name	Specifies a unique name for this entry.

Table 10-3 USSv2 Replicated Server Configuration Properties

Field Name	Description
Server Address	Specifies the IP address of the server. If not specified the default port is 9199.
Replicated Server Timeout	Specifies the amount of time the replication queue is kept active after a replicated server has gone down.
Heartbeat Time	Specifies the amount of time between heartbeat transmissions.
Heartbeat Skip	Specifies the number of missing heartbeats before a connection to a replicated server is considered down.
Bucket Load Factor	Specifies the maximum number of heartbeat intervals of outstanding buckets before replication is halted and a reconciliation is prepared.
Idle Ack Rate	When remote ack rate per heartbeat interval drops below this limit a prepared reconciliation is started.
Replicator Pool Size	Specifies the number of threads servicing outbound replication.

Once all the properties have been specified, click **OK** to continue.

END OF STEPS

11 Configuring 8950 AAA Operators

Overview

Purpose

This chapter provides information about defining administrator access to 8950 AAA. It defines different administrator roles and functions. It also provides information on how to use the SMT Operators panel.

The following topics are included in this chapter:

Administering the 8950 AAA System

Administrators for a 8950 AAA System

8950 AAA provides administrative security control over access to the SMT configuration panels, configuration files, and Admin Interface commands. You can define administrative levels for individual users.

There are four basic types of administrators for a 8950 AAA system, as follows:

Table 11-1 8950 AAA-Types of Administrators

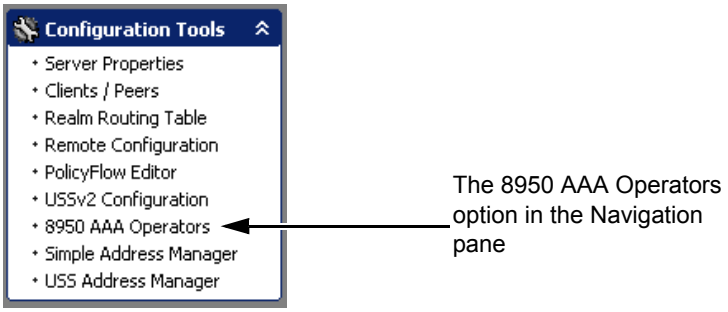
Types of Administrators	Description
Administrative User	This is the System Administrator specified during installation. The Administrative User has the following privileges: • Complete read/write access to all files • Full permissions to run all Administration interface commands for the RADIUS, USS, RMI, and Configuration servers • Control of all security files • Access to all SMT panels
Internal User	This is a special user used for internal communication between scripts and 8950 AAA Servers. The access permissions for this user are stored in the Operators file. Please refer to "Operators Tab" on page 5 for more information about Operators.
Universal State Server User	This user is used for communication within the High Availability Universal State Server (HA-USS) for replication of USS information. For more information, please refer to the High Availability-Universal State Server (HA-USS) Technical Note.
System Operator	System Operators are users that have configurable permissions to files, the Administrative Interface, and SMT panels. The Administrative User (described above) configures permissions for System Operators. The user record and its permissions can be accessed from either the Operators file or via a RADIUS Server. System Operators stored in the Operators file can be authenticated by basic password comparison as well as a variety of hashed (encrypted) passwords. Please refer to Table 11-6 on page 12 for a detailed list of supported password types.

8950 AAA Operators Panel

8950 AAA Operators

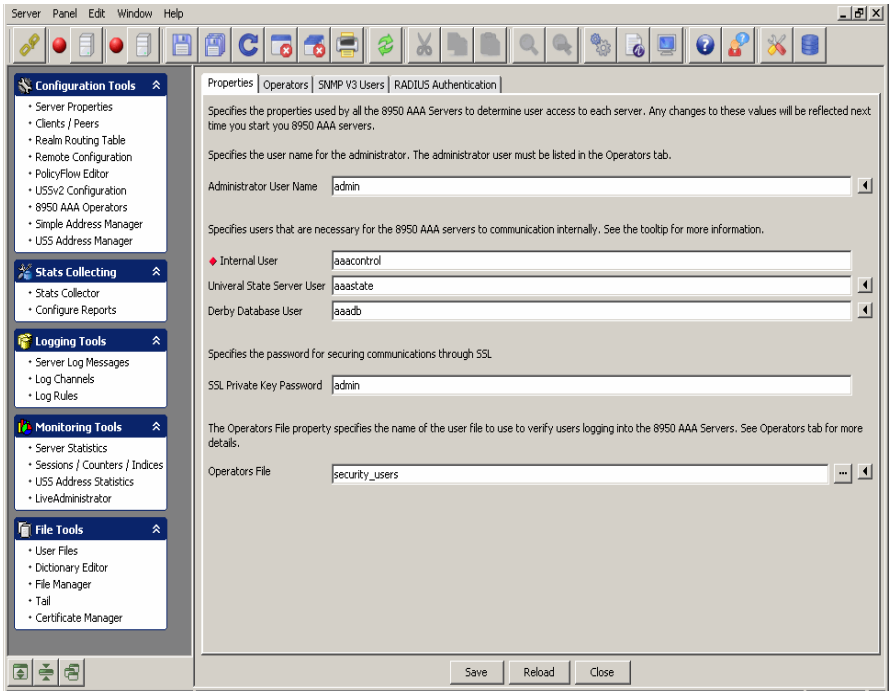
To set up the account for the Admin User or a System Operator, select **8950 AAA Operators** from the SMT Navigation Pane, as shown in Figure 11-1.

Figure 11-1 Navigation Pane-8950 AAA Operators option



Result: The **8950 AAA Operators** panel is displayed as shown in Figure 11-2.

Figure 11-2 Navigation Pane-8950 AAA Operators panel



The 8950 AAA Operators Panel, as shown in Figure 11-2, consists of four tabs, namely, Properties tab, Operators tab, SNMP V3 Users tab, and RADIUS Authentication tab. Each of these are explained in detail in the following sections.

Properties Tab

Use the fields on the Properties tab to specify values used by the 8950 AAA servers that permit access to each server. Any changes to these values will be reflected next time you start the 8950 AAA servers. By default, the Properties tab attributes are displayed in the 8950 AAA Operators Panel, as shown in Figure 11-2.

The fields are described in Table 11-2.

Table 11-2 8950 AAA Operators Panel-Properties Tab

Field Name	Description
Administrator User Name	Specifies the user name of the Administrative User / System Administrator. The administrator user must be listed in the Operators tab.
Internal User	The users necessary for the 8950 AAA server to communication internally. See the tooltip for more information. This specifies the Identifier (like a user-name) used for authenticating communications between the various 8950 AAA scripts (in the *bin* directory) and the 8950 AAA servers. This is the name of the users to lookup in the file specified in User Access File. **Important!** This user must be defined as a System Operator (that is, exist in the system Operators File defined in this Properties panel). The initial password is randomly generated and normally does not need to be changed.
Universal State Server User	The Identifier (like a user-name) used for authenticating communications between the Primary and secondary Universal State Server (USS) servers. This is only used if the High-Availability USS (HA-USS) option is installed.
Derby Database User	Specifies the user for built-in Derby database. This is also the owner of all the databases created by default (during the installation of 8950 AAA.)

Table 11-2 8950 AAA Operators Panel-Properties Tab

Field Name	Description
Administrator Password	Indicates the password for the Administrative User / System Administrator Enter a plain text password and use optional hashing (one-way encryption) on the password by clicking the button to the right of the text box and selecting the encryption method.
Operators File	The name of the user file that contains profiles of system operators

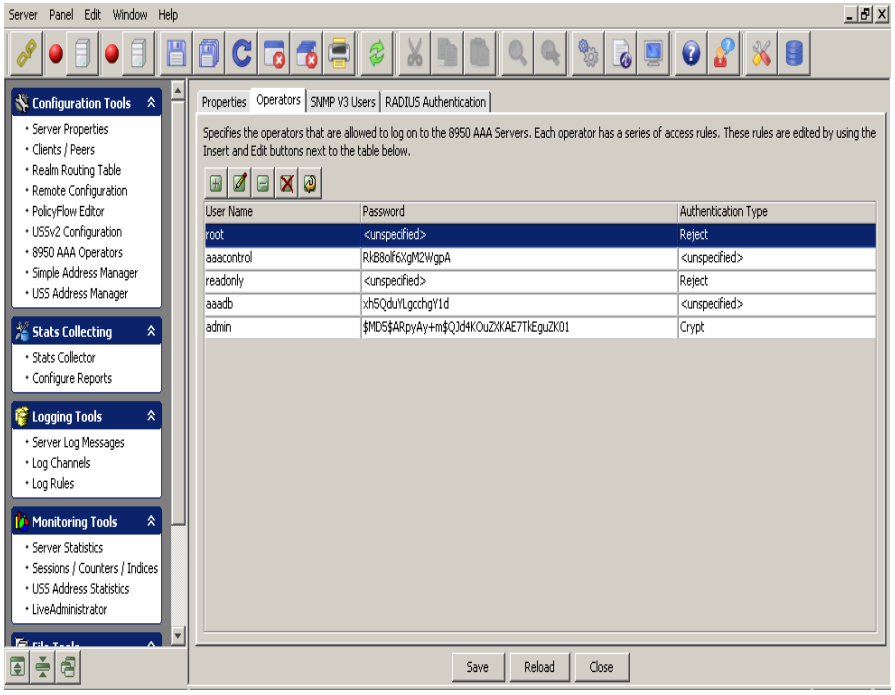
Operators Tab

The Operators tab of the 8950 AAA Operators panel lists the individual System operators who are allowed to access the 8950 AAA servers. Operators may be modified or added using the action or control buttons on the top of the panel.

Important! Panel Control functions are described in Table 3-2 on page 12.

In the 8950 AAA Operators Panel, Figure 11-2, click on the **Operators** tab. The **8950 AAA Operators–Operators tab** panel is displayed as shown in Figure 11-3.

Figure 11-3 8950 AAA Operators-Operators tab panel



The Operators tab shows three columns, as described in Table 11-3.

Table 11-3 Operators Tab-Column Headings

Column	Description
User Name	The username of this System Operator.
Password	The password for this operator, which may be plain text or hashed (encrypted.)
Authentication Type	Shows the method used to authenticate this operator. The options are described in Table 11-6 on page 12.

SNMP V3 Users

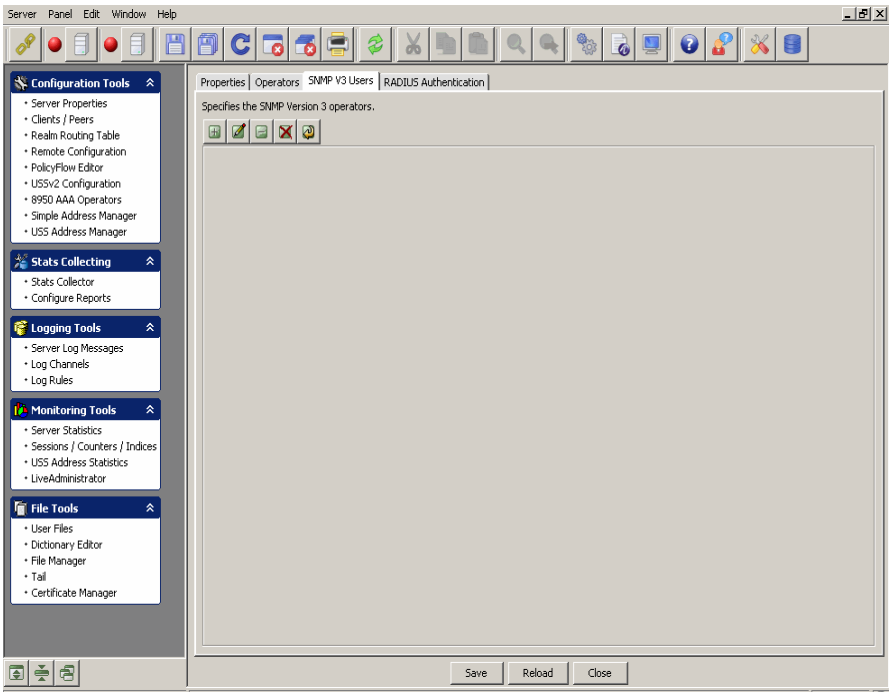
The SNMP V3 Users tab in the 8950 AAA Operators panel specifies the SNMP version 3 operators.

SNMP operator(s) information can be modified or added using the action or control buttons on the top side of the panel.

Important! Panel Control functions are described in Table 3-2 on page 12.

In the 8950 AAA Operators Panel, Figure 11-2, click on the **SNMP V3 Users** tab. The **8950 AAA Operators–SNMP V3 Users tab** panel is displayed as shown in Figure 11-4.

Figure 11-4 8950 AAA Operators-SNMP V3 Users tab panel



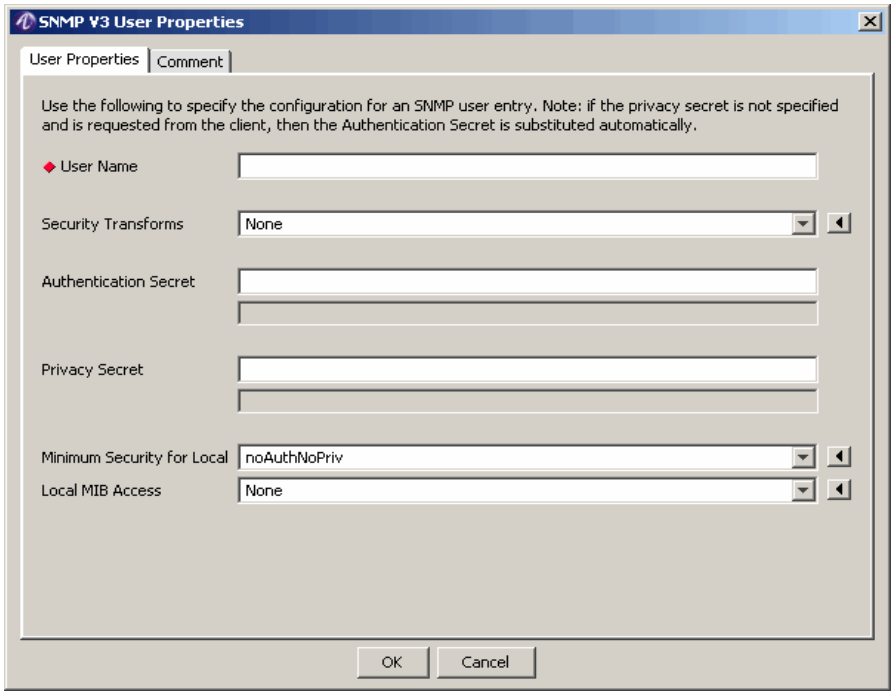
1. There are a set of action buttons on the top of this panel as shown in Figure 11-5.

Figure 11-5 Action buttons panel

2. To add a record, click the button that says + or *Insert a record*.

   Result: The **SNMP V3 User Properties** panel appears as shown in Figure 11-6.

Figure 11-6 Operators Properties-SNMP V3 User Properties panel



3. The **SNMP V3 User Properties** panel has two tabs, the **User Properties** tab and the **Comment** tab.
4. Enter the SNMP User properties in the **User Properties** tab. Table 11-4 describes the fields/attributes and descriptions in the User Properties tab. Enter any comments in the **Comment** tab dialog.

Table 11-4 SNMP V3 User Properties-User Properties Tab

Field	Description
User Name	The name of the user whose secret keys were used to possibly authenticate and encrypt the packet.
Security Transforms	This indicates whether or not messages sent or received on behalf of this user can be authenticated and if so, which authentication method to use. Also, an indication of whether or not messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use.
Authentication Secret	The localized secret key used by the authentication protocol for authenticating messages.
Privacy Secret	The localized secret key used by the privacy protocol for encrypting and decrypting messages.
Minimum Security for Local	Assigning the authentication or security level.

Table 11-4 SNMP V3 User Properties-User Properties Tab

Field	Description
Local MIB Access	Allowing the user with Read only mode or giving him permission to use any mode.

RADIUS Authentication

In addition to storing users in the Operators file, you can authenticate users using a RADIUS server. To enable RADIUS authentication, you must specify an address and secret of the RADIUS server. The RADIUS Authentication tab panel allows you to do this.

In the 8950 AAA Operators Panel, Figure 11-2, click on the **RADIUS Authentication** tab. The **8950 AAA Operators–RADIUS Authentication** tab panel is displayed as shown in Figure 11-7.

Figure 11-7 8950 AAA Operators-RADIUS Authentication tab panel

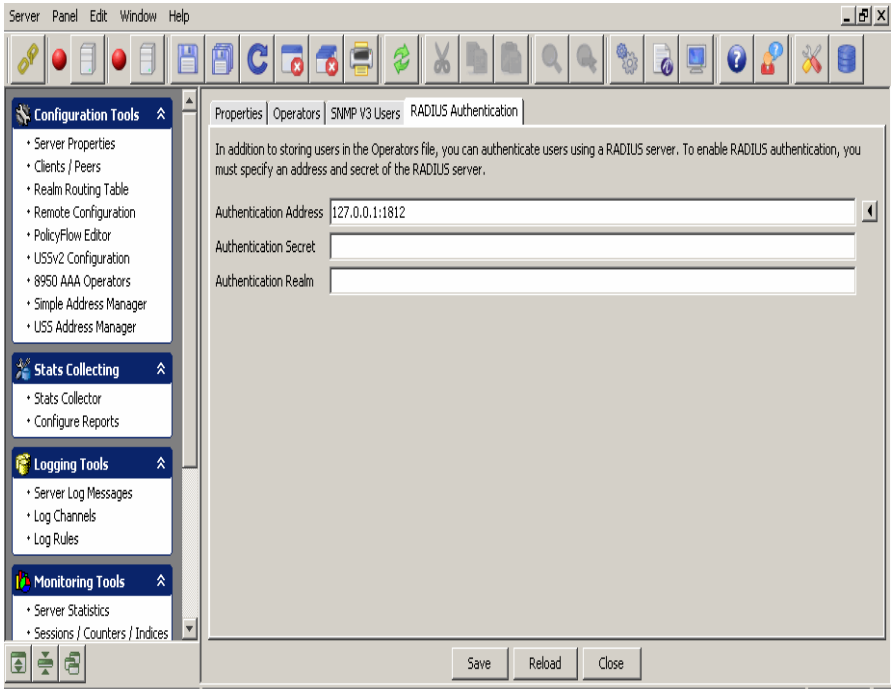


Table 11-5 describes the fields/attributes and descriptions in the RADIUS Authentication tab.

Table 11-5 Radius Authentication Tab Attributes

Access Type	Description
Authentication Address	Specifies the host IP Address and port for a RADIUS server used to authenticate System Operators. The default is the RFC defined Authentication port on the local server (127.0.0.1:1812).
Authentication Secret	Specifies the shared secret used to authenticate System Operators with a RADIUS server. If the Authentication Secret is not set, then authentication information will not be used and access to the RADIUS Server is disabled. This value is required when allowing non-admin users to login.
Authentication Realm	Specifies the Realm to append to the user when authenticating non-admin level users logging in from the SMT. This field is optional. If not specified, no Realm is used.

Adding an Operator

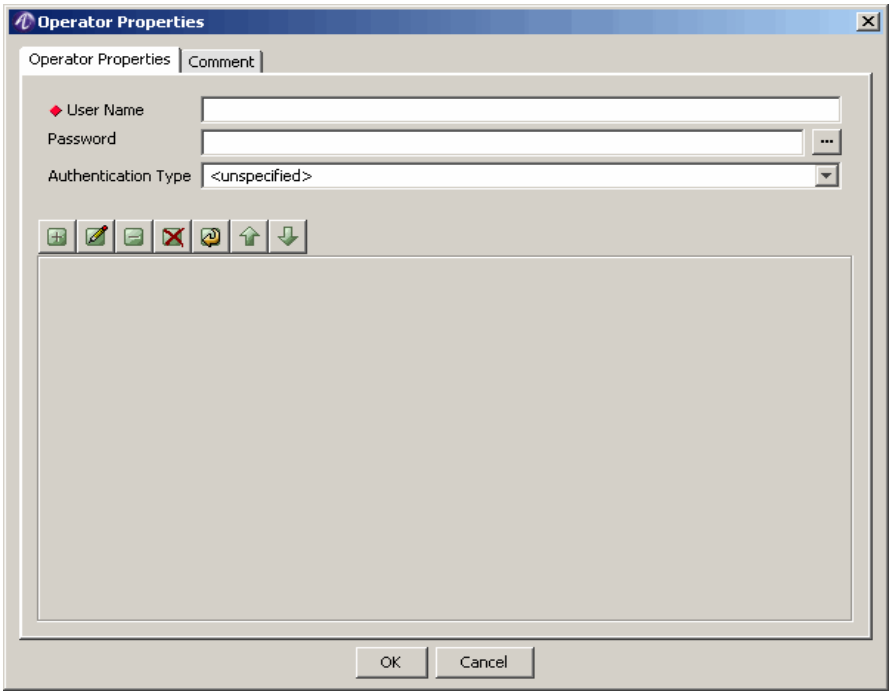
How to add an Operator

The following procedure lists the steps for creating a new System Operator.

1. From the list of action buttons panel on the top, as shown in Figure 11-5, click the button, + or *Insert a record*.

   Result: The Operator Properties Panel appears as shown in Figure 11-8.

Figure 11-8 Operators Properties-Adding Operator properties



2. Enter the name for this System Operator in the User Name field.
3. Enter a password in the Password field. To hash (a one-way encryption) the password, click the encrypt button, which is to the right of the Password field, and select an encryption styles. You may leave the password as plain text, but this may seriously compromise your system security. The following options are available:

   MD5 - Hash the password using the MD5 algorithm; the hashed password starts with `$MD5$`

   SHA1 - Hash the password using the SHA1 algorithm; the hashed password starts with `$SHA1$`

   Crypt - Hash the password using the UNIX crypt algorithm

4. From the Authentication Type drop-down list, select an appropriate authentication type as described in Table 11-6. The Authentication Type determines how password authentication should be performed. If you need an Authentication Type that is not listed in this table, then you need to configure the RADIUS Server to support it.

Table 11-6 Operator Properties-Authentication Types

Name	Description
Assert	No password is needed.
Crypt	Authenticate passwords encrypted with the UNIX crypt algorithm.
Crypt-DES	Authenticate passwords encrypted with the DES algorithm.
Crypt-MD5	Authenticate passwords encrypted with the MD5 algorithm.s
Crypt-SHA	Authenticate passwords encrypted with the SHA algorithm.
Local	Authenticate plain text passwords.
Local-Crypt	Authenticate plain text passwords encrypted with the UNIX crypt algorithm.
Local-MD4 or MD4	Authenticate plain text passwords encrypted with the MD4 algorithm.
Local-MD5 or MD5	Authenticate plain text passwords encrypted with the MD5 algorithm.
Local-Plain or Plain	Authenticate plain text passwords.
Local-SHA or SHA	Authenticate plain text passwords encrypted with the SHA algorithm.
Local-SMD5 or SMD5	Authenticate plain text passwords encrypted with the SMD5 algorithm.
Local-SSHA or SSHA	Authenticate plain text passwords encrypted with the SSHA algorithm.
None	No authentication check performed for this operator.
Passwd	Authenticate using UNIX passwd file.
Reject	Reject the request unconditionally.

5. Add one or more access rules. For more information, please refer to “Adding an Access Rule” on page 13.
6. To create a text comment for this System Operator, select the Comments tab, click the mouse pointer within the text area, and enter the comment.
7. Click **OK** to save and return to the 8950 AAA Operators panel.

   OR

   Click **Cancel** to return without saving.

Adding an Access Rule

How to add an Access Rule

You can add an Access rule from the Operators tab. In the Operator Properties Panel, as shown in Figure 11-8, click on the + or the Insert a Record action button. The Access Item Configuration dialog appears as shown in Figure 11-9.

Each access rule consists of three components:

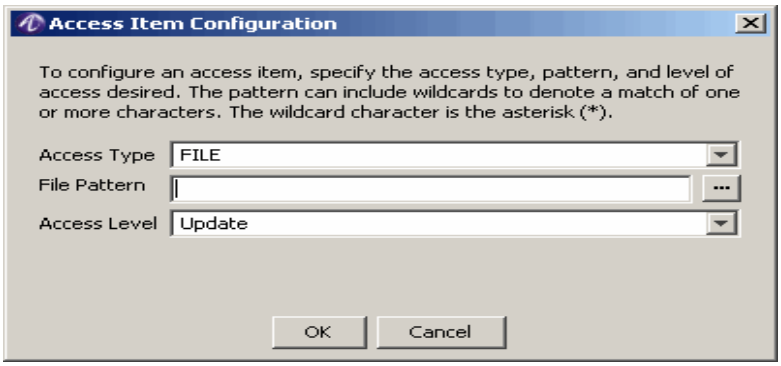
- *Access Type* defines the type of 8950 AAA object to which this rule applies.
- *File, Command, or Rule Pattern* names the object or objects to which this Access Rule applies.
- *Access Level* defines the type of access this System Operator has to the objects.

To add an access rule, perform the following steps:

- From the Operator Properties panel (Figure 11-8 on page 11), click the button that has + or the *Insert a record* button.

  Result: The Access Item Configuration dialog appears as shown in Figure 11-9.

Figure 11-9 Access Item Configuration Dialog



8. From the Access Type drop-down list, select an access type for this rule. There are three access types available, namely, **File**, **Command**, and **Role**. They are described in Table 11-7.

Table 11-7 Access Rules-Access Type Component

Access Type	Description
File Access Type	Controls access to configuration files. Also controls access to the SMT panels that manage data in the selected file.
Command Access Type	Controls access to administrator interface commands.

Table 11-7 Access Rules-Access Type Component

Access Type	Description
Role Access Type	Controls access to Remote Method Invocation (RMI). Generally applies to SMT access permissions to RADIUS and state servers and by the HAUSS during replication.

Result: The selected Access Type determines the Pattern and Access Level fields.

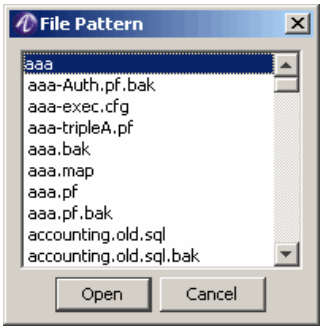
9. Enter a value for the Pattern.

   When the Access Type is **FILE**, then **File Pattern** appears as the second field, as shown in Figure 11-9, above.

   In the File Pattern text field, type a name or a limited wildcard pattern. For example, the File Pattern ***_methods** would match auth_methods and acct_methods.

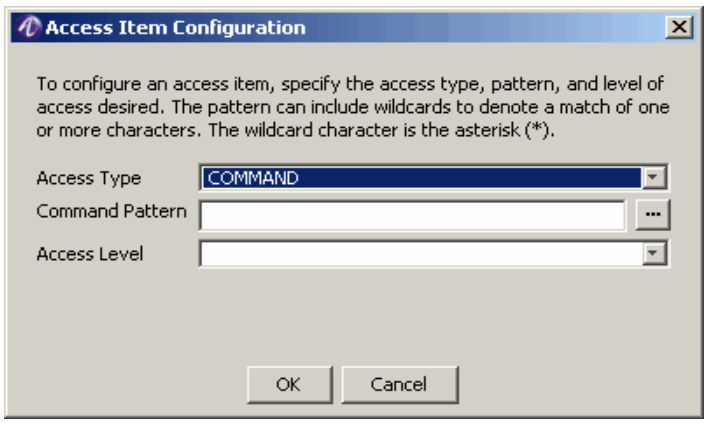
   You may also click the File Pattern button, at the right of the field, to select a commonly used name for the selected Access Type. Select from the File Pattern dialog as shown in Figure 11-10.

Figure 11-10 File Pattern Dialog



If the selected Access Type is **Command**, then **Command Pattern** appears as the following field, as shown in Figure 11-11.

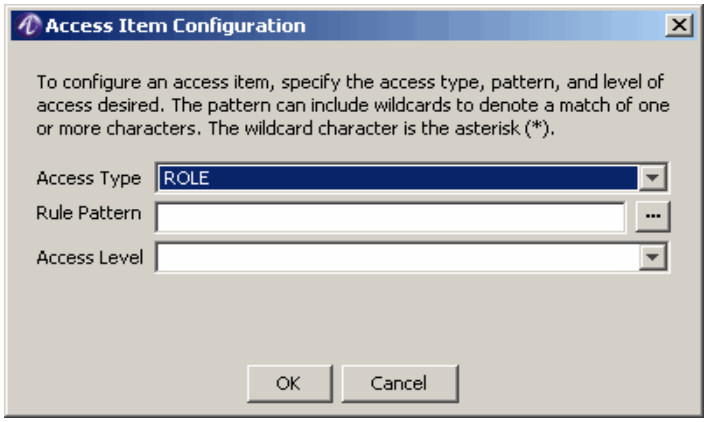
Figure 11-11 Access Item Configuration Dialog-Command Access Type



As described above for File Pattern, enter a value for Command Pattern using either a name, a limited wildcard pattern, or the button to the right of the field.

If the selected Access Type is **Role**, then **Rule Pattern** appears as the following field, as shown in Figure 11-12. Enter a value for the Rule Pattern in the same way as described for File Pattern and Command Pattern.

Figure 11-12 Access Item Configuration Dialog-Role Access Type



1. Select an appropriate access level from the Access Level drop-down list.

   Like the File Pattern, the Access Level list values depend upon the selected Access Type as shown in Table 11-8.

Table 11-8 Access Rules-Access Type and Access Level Components

Access Type	Access Level	Description
File	Update	Allows both read and write access
	Read	Allows read only access
	None	Denies access

Table 11-8 Access Rules-Access Type and Access Level Components

Access Type	Access Level	Description
Command	On	Allows command execution
	Off	Denies command execution
Role	On	Allows access to a particular role for methods execution
	Off	Denies access for method execution

2. After selecting the access level, the access rule is complete.

   Click **OK** to save and return to the Operator Properties tab

   OR

   Click **Cancel** to return without saving.

   Result: The Operator Properties tab appears with the new rule.

   Add additional Access rules as necessary.

   Important! Access Rules are applied in order, the first matching rule is selected. You should place more general rules near the bottom and more specific rules near the top of the list of rules.

Modifying a System Operator

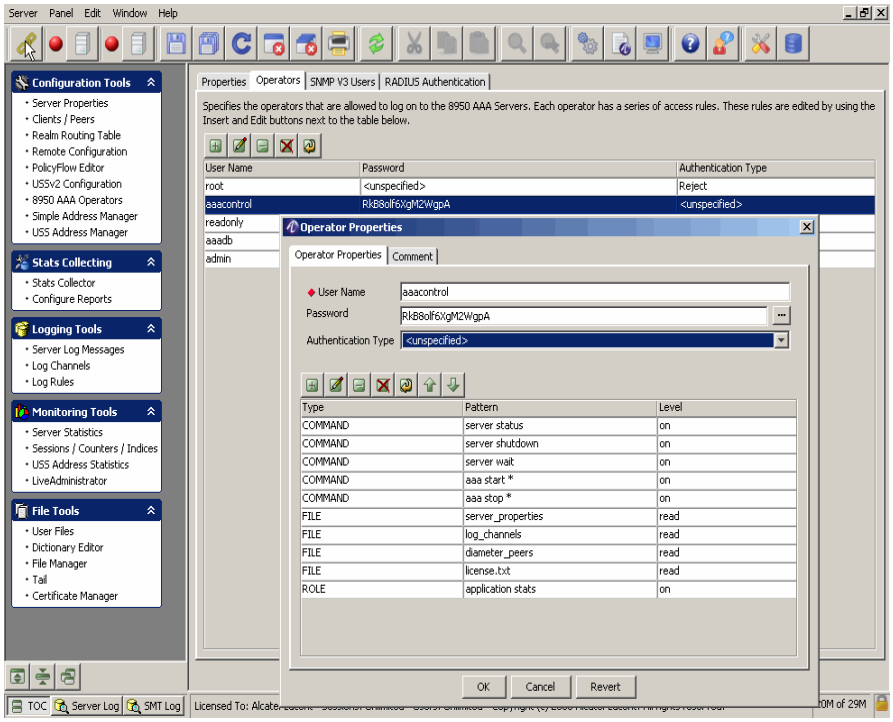
How to modify a System Operator

The following procedure lists the steps for changing the attributes of a System Operator.

1. From the Operators tab on the 8950 AAA Operators panel, select the operator to be modified.
2. Double click on the operator or select the *Edit selected record* panel control button.

   Result: The Operator Properties screen appears with the current information about the selected operator as shown in Figure 11-13.

Figure 11-13 Modifying a System Operator



3. Modify the existing User name, Password, or Authentication Type.
4. Modify any rule by selecting it and double clicking on the rule or by clicking the *Edit selected record* action button that appears to the top of the list of access rules.

   Result: Current data about the rule appears and this data is editable.

5. Save all desired modifications before returning to the Operators panel.

END OF STEPS

12 Configuring Simple Address Manager

Overview

Purpose

This section discusses the tools that are used for the configuration and management of address pool by the Simple Address Manager. Simple Address Manager provides dynamic address pool management.

The following topic(s) is/are included in this chapter:

Simple Address Manager Configuration

Simple Address Manager Panel

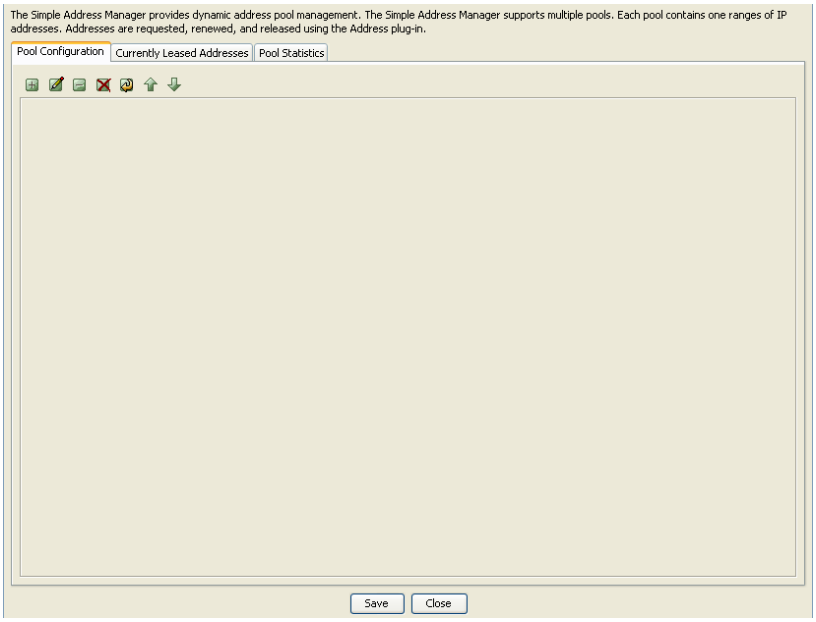
The Simple Address Manager configures and manages the address pool. It supports multiple pools. Each pool in a Simple Address Manager contains a range of IP addresses. Addresses are requested, renewed, and released using the Address plug-in.

To display the Simple Address Manger panel, use the SMT Navigation Pane to select **Simple Address Manger** under Configuration Tools, as shown in Figure 12-1.

Figure 12-1 Navigation Pane-Simple Address Manager

The Simple Address Statistics panel appears as shown in Figure 12-2.

Figure 12-2 Simple Address Manager Panel



The Simple Address Manager contains three tabs:

- Pool Configuration
- Currently Leased Addresses
- Pool Statistics

Pool Configuration tab

The Simple Address Manager panel with the Pool configuration tab selected is shown in Figure 12-4 selected.

A set of action buttons, as shown in the Figure 12-4 are also present in the Pool Configuration tab.

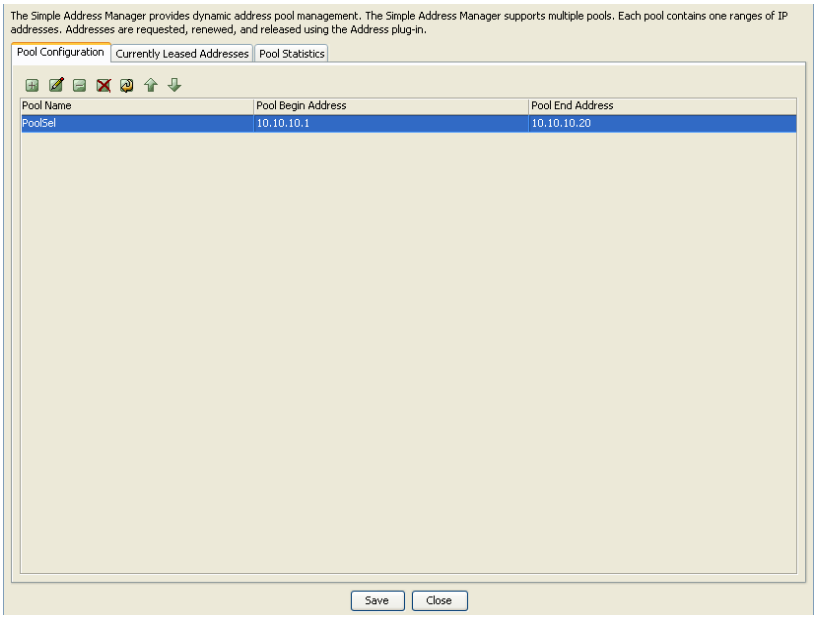
Figure 12-3 Simple Address Manager-Action Buttons

The action buttons allow you to perform the following actions:

- Insert a record
- Edit a record
- Delete a record
- Delete all records
- Make a copy of selected records
- Move selected record up

- Move selected record down

Figure 12-4 Simple Address Manager: Pool Configuration tab

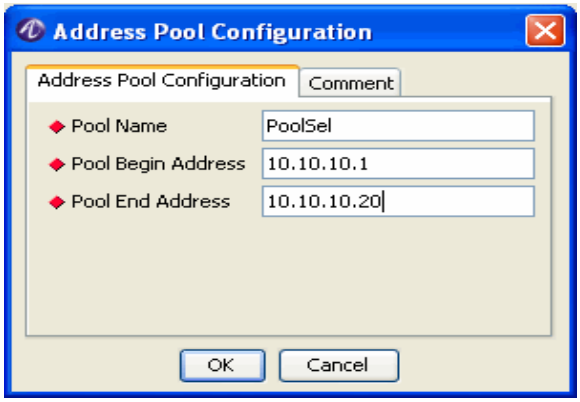


Click on the  action button. Address Pool Configuration panel is displayed as shown in the Figure 12-4. This screen allows you to add records to the Address Pool Configuration.

Using the Pool Configuration tab to add a record

The Pool Configuration panel allows you to add a record and enter information in the required fields as shown the Figure 12-5

Figure 12-5 Simple Address Manager-Address Pool Configuration Panel



Click the Comment tab to enter your comments if any and click OK.

The pool entry added is displayed on the Simple Address Manager panel as shown in the Figure 12-4.

Currently Leased Addresses tab

The Figure 12-6 displays the Simple Address Manager panel with the Currently Leased Addresses tab selected. This screen displays the details of IP addresses that have been leased.

Figure 12-6 Simple Address Manager-Currently Leased Addresses tab

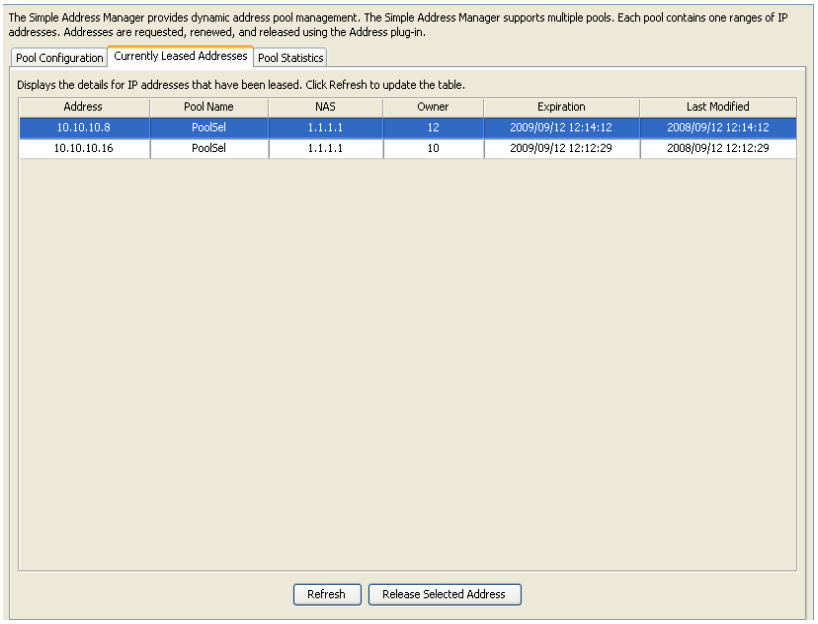


Table 12-1 describes the different attributes/properties of the leased IP address.

Table 12-1 Currently Leased Addresses tab-Properties

Attributes	Description
Address	Leased IP address.
Pool Name	Pool to which the leased IP address belong.
NAS	The Network Access Server IP address.
Owner	The Network Access Server port IP address (client to which it is leased).
Expiration	Lease expiration time.
Last Modified	Last modification date and time.

Click **Refresh** to update the table and **Release the Selected Address** to remove it from the list by sending it back to the pool.

Pool Statistics tab

The Figure 12-7 displays the Simple Address Manager panel with the Pool Statistics tab selected. This screen displays the available addresses for each pool.

Figure 12-7 Simple Address Manager-Pool Statistics tab

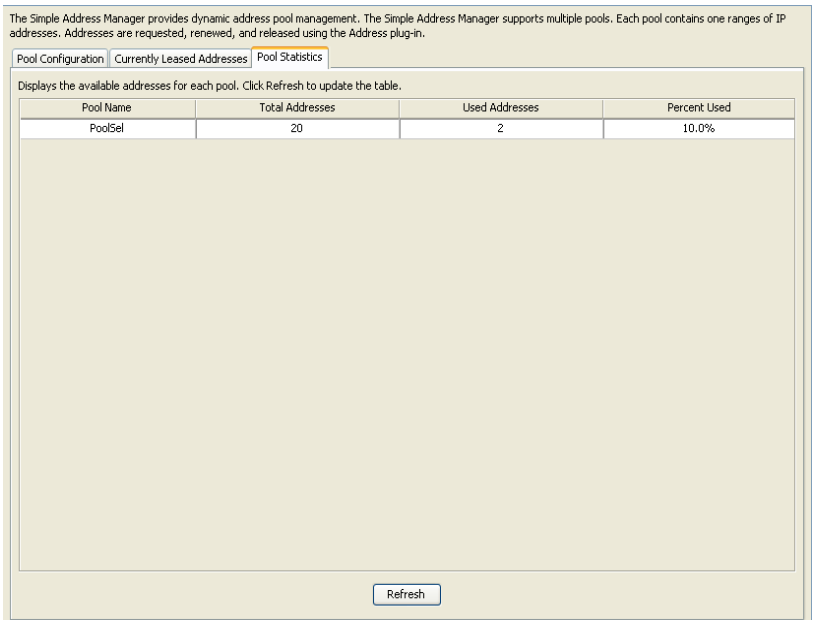


Table 12-2 describes details of the pool to which the leased IP address belongs.

Table 12-2 Pool Statistics tab-Properties

Attributes	Description
Pool Name	Pool to which the leased IP address belongs.
Total Addresses	Total number of addresses present in the pool.
Used Addresses	Number of addresses used from the pool.
Percent Used	Percentage of addresses used from pool.

Click **Refresh** to update the table.

END OF STEPS

13 Configuring USS Address Manager

Overview

Purpose

This section discusses the tools that are available for the configuration and management of address pools of 8950 AAA, using Universal State server.

The following topics are included in this chapter:

USS Address Manager Configuration

USS Address Manager Panel

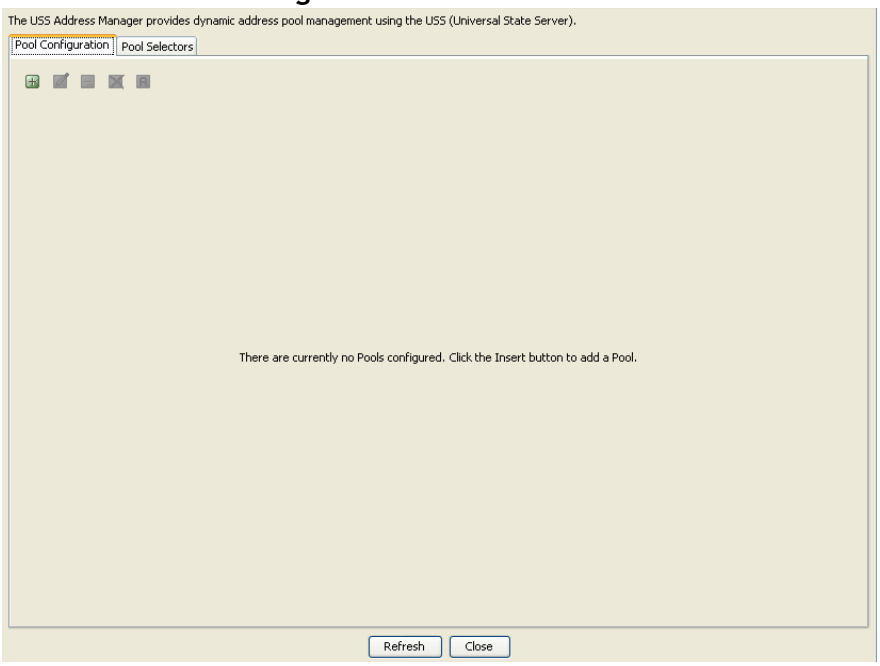
The USS Address Manager provides dynamic address pool management using the Universal State Server.

To display the USS Address panel, use the SMT Navigation Pane to select **USS Address Manager** under Configuration Tools, as shown in Figure 13-1.

Figure 13-1 Navigation Pane-USS Address Manager

The USS Address Manager Panel appears as shown in Figure 13-2.

Figure 13-2 USS Address Manager Panel



The USS Address Monitor panel contains two tabs; **Pool Configuration** and **Pool Selectors**.

A set of action buttons, as shown in the Figure 13-3 are also present in the USS Address Monitor panel.

Figure 13-3 USS Address Manager-Action Buttons

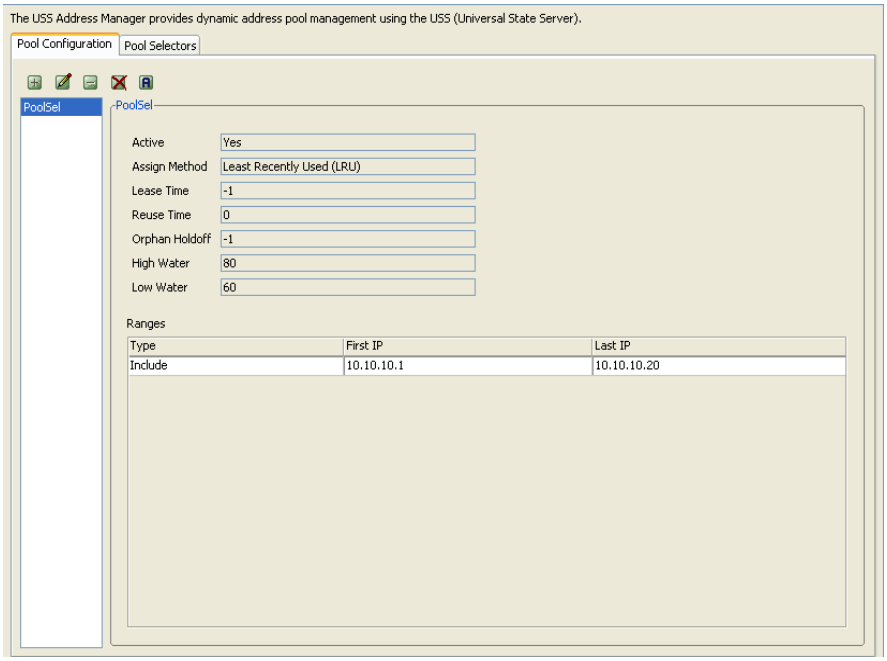
These action buttons allow you to perform the following actions:

- Insert a record
- Edit a record
- Delete a record
- Delete all records
- Toggle the activation of selected pool (Not seen for the Pool Selector tab)

Using the Pool Configuration tab in USS Address Manager Panel

The USS 8950 AAA Address Manager panel with the Pool configuration tab selected is shown in Figure 13-4.

Figure 13-4 USS Address Manager-Pool Configuration tabl

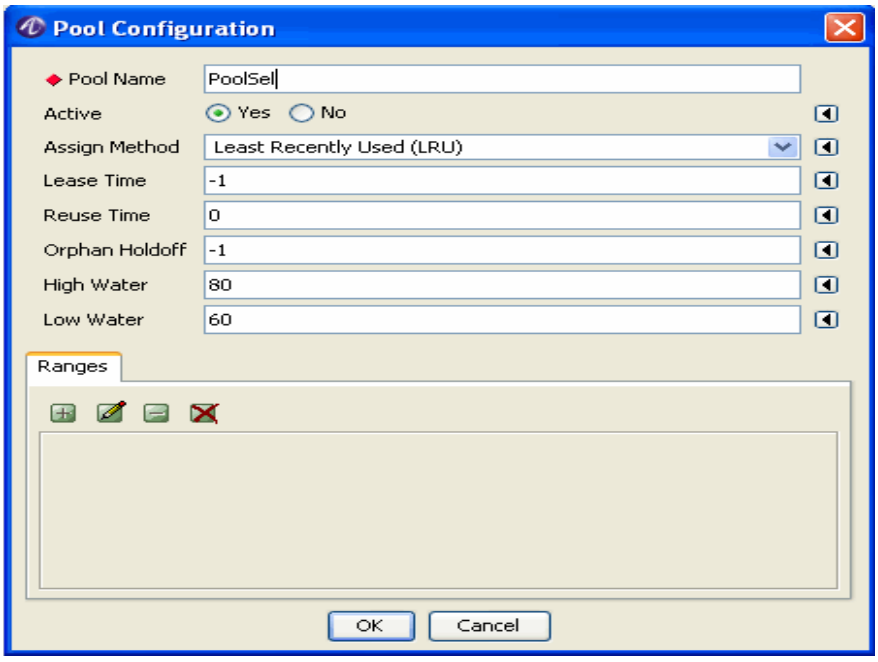


On the USS Address Manager panel, click the Pool Configuration tab. Click on the  action button. Pool Configuration panel is displayed as shown in Figure 13-2. This panel allows you to add or insert record to the Pool Configuration.

Using the Pool Configuration tab to add a record

The Pool Configuration panel allows you to add a record and enter information in the required fields as shown the Figure 13-5

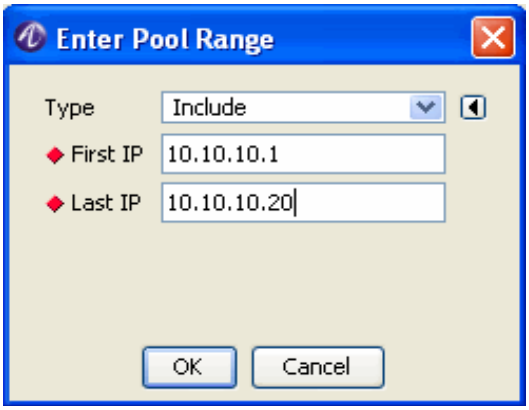
Figure 13-5 USS Address Manager-Pool Configuration Panell



On the below portion of Pool Configuration panel, there is a Range panel. Use the Range panel to specify the range of IP addresses.

On the Range panel, click on the  action button. Enter Pool Range screen is displayed as shown in Figure 13-6.

Figure 13-6 USS Address Manager-Enter Pool Range Panell



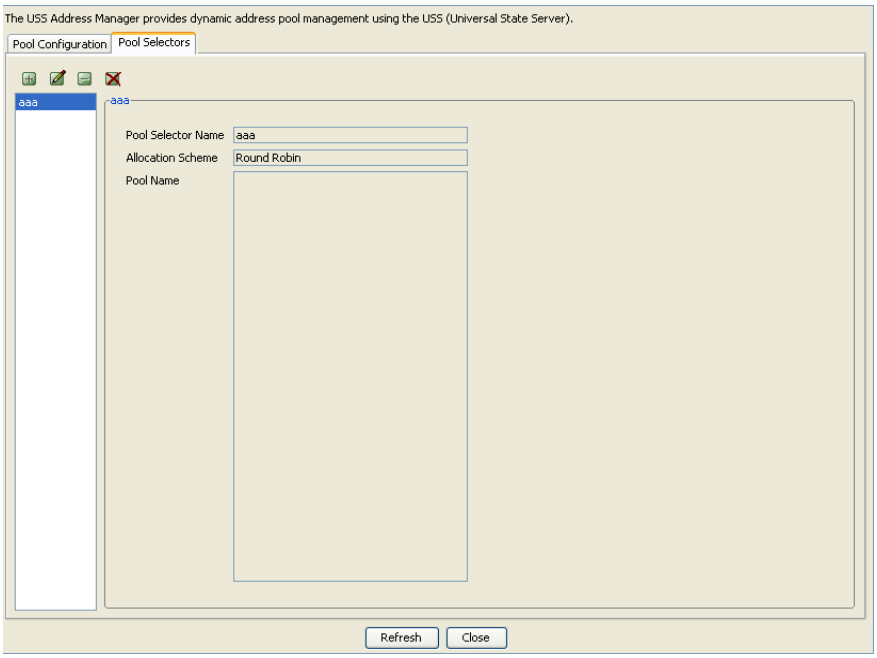
Select the required Type (Inclusion or exclusion) and enter the first and second IP addresses. Click OK. The new record is added. The Figure 13-4 displays the attributes of the Pool selected on the top portion and the range on the bottom portion.

Use the Edit or Delete action buttons to alter the records.

Using the Pool Selectors tab in USS Address Manager Panel

The USS Address Manager panel with the Pool Selector tab selected is shown in Figure 13-7 selected.

Figure 13-7 USS Address Manager-Pool Selector Panell

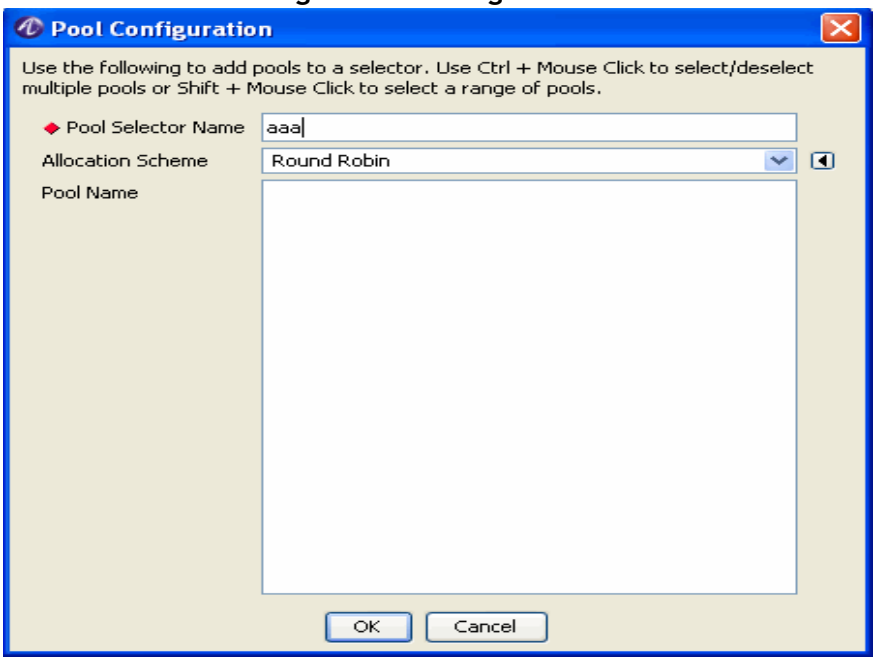


On the USS Address Manager panel, click the Pool Selector tab. Click on the  action button. Pool Configuration panel is displayed as shown in Figure 13-2. This panel allows you add or insert record to the Pool Configuration.

Using the Pool Selector tab to add a record

The Pool Configuration panel allows you to add a record and enter information in the required fields as shown the Figure 13-8

Figure 13-8 USS Address Manager-Pool Configuration Panell



Enter the Pool Selector Name and select the required allocation scheme. The pool name is displayed in the Pool Name field. Click OK to add the record. The record added is displayed in the Figure 13-7.

Use the Edit or Delete action buttons to alter the records.

END OF STEPS

Part II: Stats Collecting Navigation Pane

Overview

Purpose

This part consolidates the chapters related to Configuration Tools in the SMT Navigation pane.

Contents

This part includes the following chapters.

14 Stats Collector

Overview

Purpose

This section discusses about the various parts of 8950 AAA tool that collects statistical information of 8950 AAA.

The following topics are included in this chapter:

The Stats Collector

Overview

The collector is the part of 8950 AAA that collects statistical information about various parts of 8950 AAA. The Collector has Groups, which are listed on the left. Each group contains a list of statistics that you can enable.

To start the collecting, select the desired group from the list on the left, then enable the parts of the group you want to gather. Once the Policy Server has collected some data, use the Configure Reports panel to build reports and graphs.

The **Stats Collector** panel has two panels that are located under the SMT Navigation Area, under **Stats Collecting**:

- The left section that displays information about the list of available groups.
- The right section displays information about the selected item.

Stats Collector Panel

About Stats Collector Panel

The Stats Collector panel provides the ability to monitor the following aspects of 8950 AAA server operations:

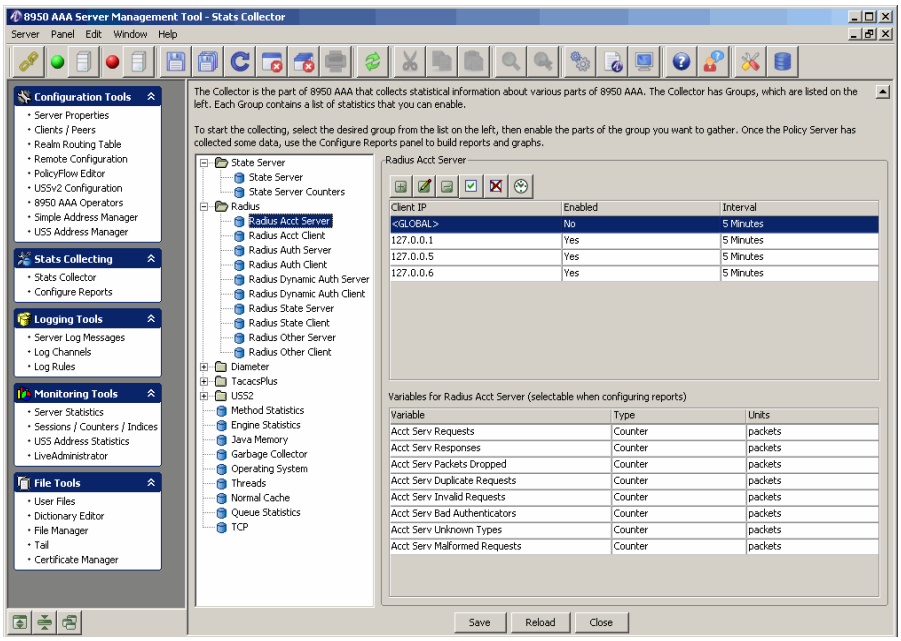
- Add, Modify, or Delete Client/Peer IP information
- Enable or Disable instances
- Change intervals for selected instances

To display the Stats Collector panel, use the SMT Navigation Pane and select **Stats Collector** under **Stats Collecting**, as shown in Figure 14-1.

Figure 14-1 Navigation Pane-Stats Collector

The Stats Collection Panel appears as shown in Figure 14-2.

Figure 14-2 Stats Collector Panel



This panel contains two sections as follows:

- The left section contains a list of groups like the State Server, Radius, Diameter, TacacsPlus, USS2, and so on. Each of these group contains a list of statistics associated with them.

- The right section has two parts. The top portion displays information about the selected group/item. It allows you to add, modify, or delete client/peer IP instance information and allows you to change the interval for these instances and to either enable/disable these instances.
  The bottom portion displays the information about the variables for the selected group/item. This is only for information and is read-only.

As shown in Figure 14-2, the statistics that you can modify or enable are categorized according to the groups that they belong to.

The right section of Figure 14-2 displays statistical information on Radius Acct Server and information on the variables for the Radius Acct Server.

Use the action buttons in the top of the right section to modify the contents of the statistical information. The function of each button is listed in Table 14-1.

Table 14-1 Stats Collector Panel-Action Buttons

Name	Description	Icon
Insert	Add a record in the current panel after the selected row. If no row is selected, the record is inserted at the end of the list.	
Edit	Edit the values for the selected record.	
Delete	Removes the selected row from the active view.	
Enable	Displays an option to either Enable the selected instance or Enable all instances in the view.	
Disable	Displays an option to either Disable the selected instance or Disable all instances in the view.	
Change Interval	Allows you to set or change the interval time for the selected instance or all the instances in the view.	

- Use the control buttons at the bottom of the screen to manage the available views. They are described in Table 14-2.

Table 14-2 View Control Buttons

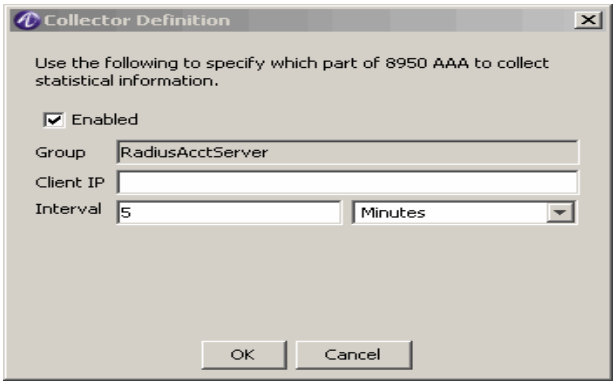
Name	Description
Save	Saves the information in the 8950 AAA database.
Reload	Reloads the Stats collector information to the 8950 AAA database.
Close	Closes the Stats Collector panel.

Using the Stats Collector Action buttons

The action buttons on the top of the right side of the Stats Collector panel allows you to perform the actions specified in Table 14-1.

1. To add Stats Collector information, select the group in which you want to add an entry and click the Insert button. The Collector Definition screen is displayed as shown in Figure 14-3.

Figure 14-3 Stats Collector-Insert Information



2. Enter Client IP, Interval (select Milliseconds, Seconds, Minutes, or Hours for Interval). Click **OK** to update the Stats Collector information that you entered.
3. To edit the Stats Collector information, select the required entry in the desired group, that you want to edit and click the Edit button. The Collector Definition screen, as shown in Figure 14-3, appears with the existing values. You can modify the information that can be edited and click **OK** to update the Stats Collector information.
4. To delete Stats Collector information, that belongs to a group, select the entry to be deleted and click the Delete button. The selected entry will be deleted.
5. To enable the selected instance or to enable all the instances in the selected group, click on the Enable button. It gives you an option to either enable the selected instance/entry or to enable all the instances/entries in the group. Choose the required option. The instance(s) will be enabled as selected.

6. To disable the selected instance or to disable all the instances in the selected group, click on the Disable button. It gives you an option to either disable the selected instance/entry or to disable all the instances/entries in the group. Choose the required option. The instance(s) will be disabled as selected.
7. To change the interval time for the selected instance or for all the existing instances in the selected group, click on the Change Interval button. It gives you an option to Set the time for the Selected instance or to Set the time for all the instances in the group. Choose the required option and set the time from the available list. The Interval time for the instance(s) will be set as selected.

END OF STEPS

15 Configuring Reports

Overview

Purpose

This section discusses about the reports configurator for the 8950 AAA tool.

The following topic(s) is/are included in this chapter:

The Configure Reports Panel

About Reports Configurator

The Configure Reports panel provides the ability to configure and generate reports from the statistical data collected by the 8950 AAA.

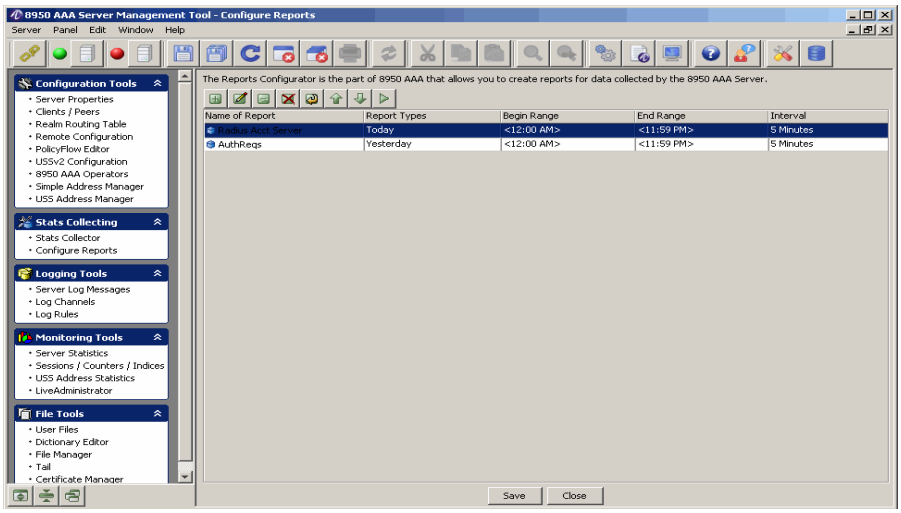
The Reports Configurator is the part of 8950 AAA that allows you to create reports for data collected by the 8950 AAA.

To display the Configure Reports panel, use the SMT Navigation Pane and select **Configure Reports** under **Stats Collecting**, as shown in Figure 15-1.

Figure 15-1 Navigation Pane-Configure Reports

The Configure Reports (or Reports Configurator) Panel appears as shown in Figure 15-2.

Figure 15-2 Configure Reports Panel



The Configure Reports panel (Figure 15-2) contains five columns and a set of Action Buttons that appear at the top of the screen, as shown in Figure 15-3.

Figure 15-3 Configure Reports Panel- Action buttons

These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down
- Run selected report

You can perform any of the required actions using these action buttons.

1. To Insert a record, click the **Add a record** action button,  . The **Configure Report** panel is displayed as shown in Figure 15-4. This panel allows you to add a record/report and enter required information to configure a report as shown in Figure 15-4.

Figure 15-4 Configure Reports Panel- Add record

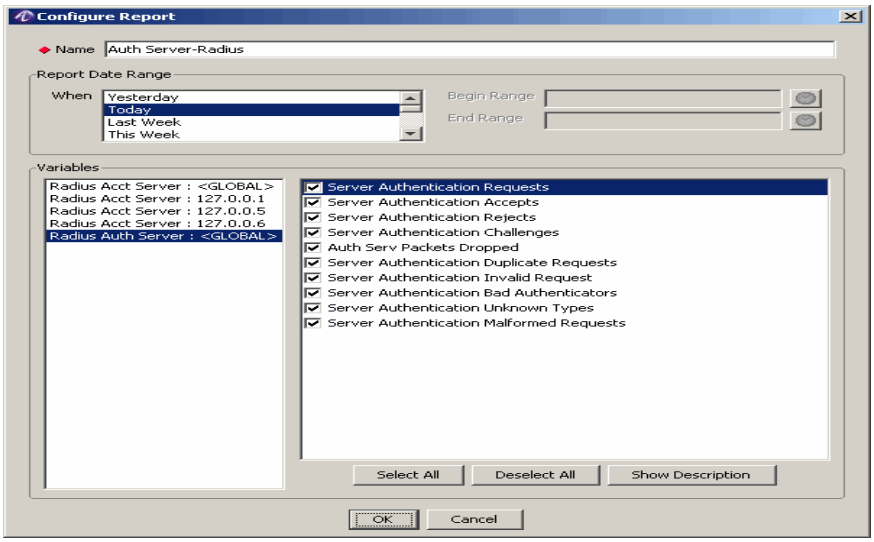


Table 15-1 explains each of these fields and the field descriptions. There are two sets of properties that you need to specify in this screen.

Table 15-1 Configure Reports Panel-Properties

Field Name	Description
Name	The name of the Report.
Report Date Range	
When	The day on which the report is created.
Begin Range	The time/date range to begin the report. **Important!** This is taken by the system and is not editable.
End Range	The time/date range to end the report. **Important!** This is taken by the system and is not editable.
Variables	
Variables	Displays a list of available groups on the left side. Also displays a list of appropriate variables for the selected group on the right side.

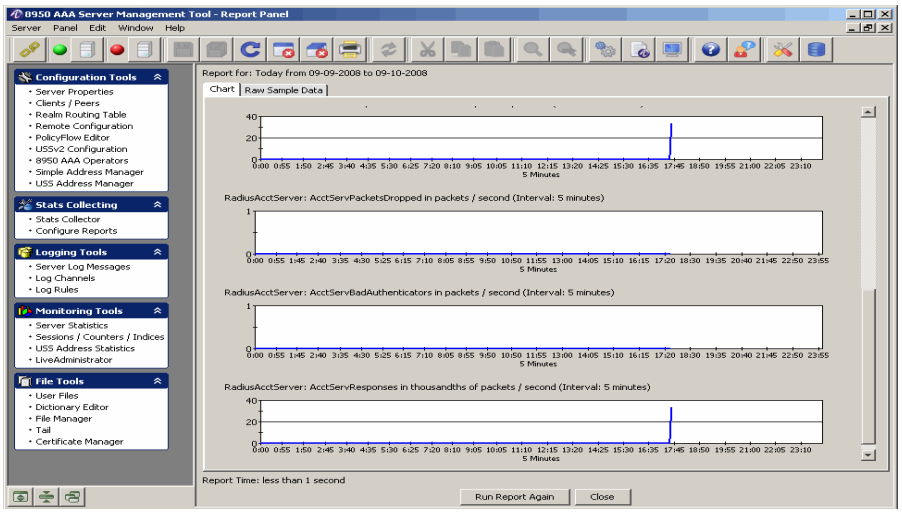
Use the buttons at the bottom of the screen to select or deselect the listed variable(s). They are described in Table 15-2.

Table 15-2 Configure Reports Panel-Buttons

Name	Description
Select All	Selects all the displayed variables.
Deselect All	Deselects all the displayed variables.
Show Description	Shows description about the selected variable.

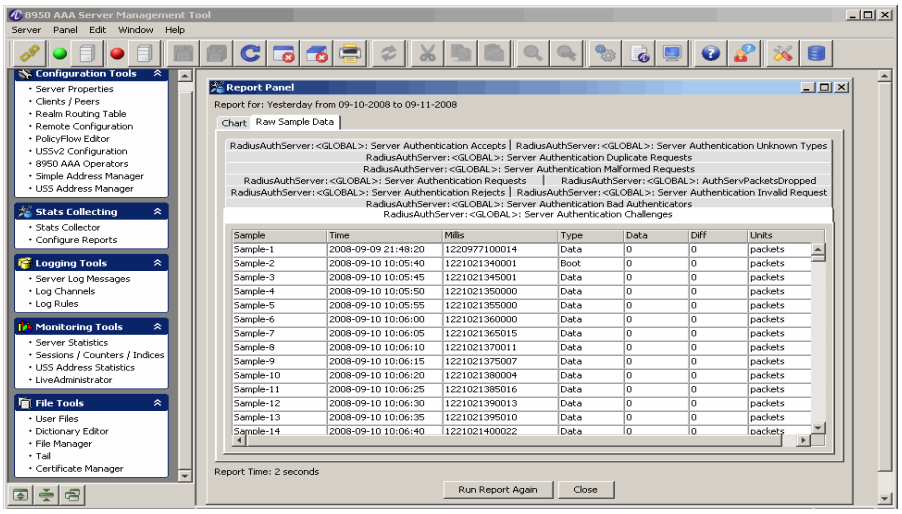
2. Click OK to add the record.
3. To edit the information about a configured report, select the required entry and double click on it or click the **Edit a record** action button,  . The **Configure Report** panel is displayed as shown in Figure 15-4. You can modify the information that can be edited and click **OK** to update the configured report information.
4. To delete a configured report information, select the entry to be deleted and click the **Delete record** action button. The selected entry will be deleted.
5. To delete all the configured reports in the panel, click the **Delete All** action button. A confirmation dialog is displayed asking you to confirm to delete all the records. Click **Yes** to delete all the records or click **No** to exit the action and come out of the dialog.
6. To make a copy of an existing report, click the **Make a copy of the selected record** action button. The **Configure Report** panel is displayed as shown in Figure 15-4. Edit the name of the Report and click OK to add a copy of the existing report.
7. To move a report up, click the Up arrow key action button or the **Move selected record up** action button.
8. To move a report down, click the Down arrow key action button or the **Move selected record down** action button.
9. To run a report, click the **Run Selected Report** action button. The Report Panel is displayed, as shown in Figure 15-5.

Figure 15-5 Report Panel-Chart tab



This has two tabs. The **Chart** tab shows the report in graphical format as shown in Figure 15-5. The **Raw Sample Data** tab shows the report in the sequenced format, as shown in Figure 15-6.

Figure 15-6 Report Panel-Raw Sample Data tab



10. Click **Run Report Again** button to run the report once again.
11. Click **Close** to close the Report Panel and go back to the **Configure Report** panel, as shown in Figure 15-4.

END OF STEPS

Part III: Logging Tools Navigation Pane

Overview

Purpose

This part consolidates the chapters related to Logging Tools in the SMT Navigation pane.

Contents

This part includes the following chapter(s).

16 Message Logging

Overview

Purpose

The 8950 AAA Server Management Tool allows the user to manage how and when a server can log messages. This section describes the messages and how to control message logging.

The following topics are included in this chapter:

8950 AAA Message Overview

Message Overview

The 8950 AAA server creates and writes messages for actions that occur during initial startup, while running, and while shutting down. These messages have the basic form shown below:

Important! The contents of log messages can be highly customized in 8950 AAA. The description presented here covers the default format. If you have made changes to your logging channels, your output may look different.

2005/02/26 14:15:48.287 (NOTICE) Licensed for 12 clients

As shown in the example, the contents of a log message contains the following:

- *Timestamp*

  The time the server logs the message. By default, the timestamp includes the date and time in the following format:

  ```
  YYYY/MM/DD HH:MM:SS.mmm
  ```

  where mmm represents milliseconds.

  For example: `2005/02/24 09:10:57.760`

- *Area*

  The functional area of the 8950 AAA software that generated the message. Usually, this information follows the timestamp and is contained within angle brackets (< >). For example: `<nr.setup>`

- *Level*

  The log level of the message. The log level defines the severity of the action that triggered the message. For example `(NOTICE)`.

  Refer to the table below for a list of 8950 AAA log levels.

- *Message*

  The actual message the server logs when the action occurs.

Messages are logged by 8950 AAA when specific conditions are met. These conditions may be tied to the occurrence of a small set of common request processing actions (request accept, request reject, etc.), or to custom user defined conditions. Log messages may also be generated by instructions in a PolicyFlow program. By default, messages are logged to a text file named policy.log. This file can be located within your run directory.

Important! Logging and Performance. While logging is essential to good server management, it can also have a negative impact on system performance. As a general rule you should try to log the minimum number of messages possible that will yield the level of log detail you require for your operations.

Logging Tools

About Logging Tools

The Logging Tools Section of the Navigation Pane provides three panels for controlling server log message output, as listed in Figure 16-1.

- The *Server Log Messages panel* controls a set of log messages keyed to the common request processing actions.
- The *Log Channels panel* manages the destinations available for 8950 AAA log message output.

- The *Log Rules panel* defines basic criteria that 8950 AAA uses to determine which messages to log and the channel to which the message should be logged.

Figure 16-1 Logging Tools Section in the Navigation Pane

The following sections provide more information on the panels, their components, and their functionality.

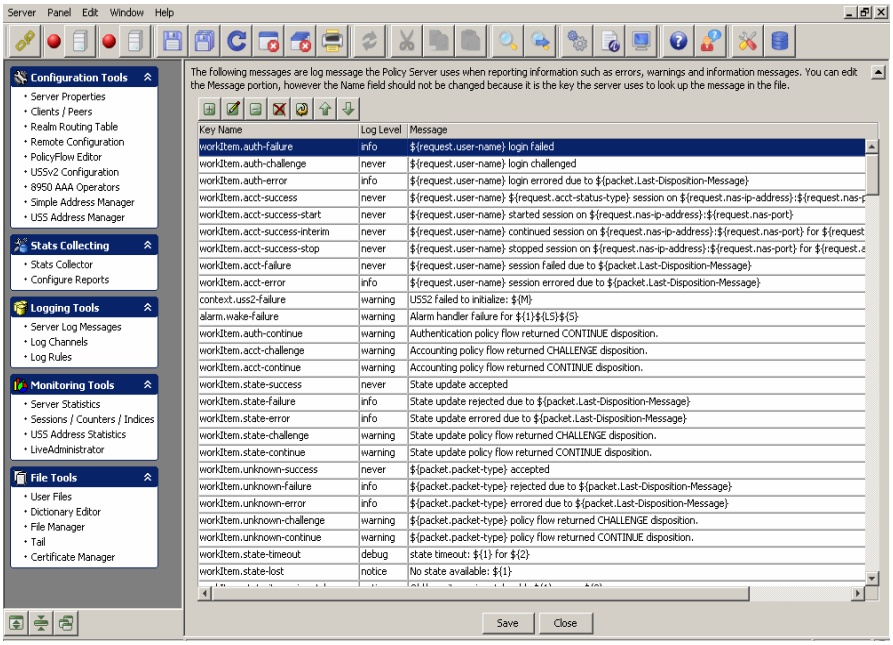
Server Log Messages

About Log Messages

Select **Server Log Messages** from the **Logging Tools** section on the Navigation pane. The *Server Log Messages* panel is displayed as shown in Figure 16-2.

This panel contains all the existing server log messages in SMT. It allows you add new log messages, edit the existing messages, delete messages, and copy the existing message, and move the messages up or down.

Figure 16-2 Server Log Messages Panel



The messages displayed are log messages the Policy Server uses when reporting information such as errors, warnings and information messages. You can edit the Message portion. However, the Name field should not be changed because it is the key the server uses to look up the message in the file.

Action buttons in the Server Log Messages section

The **Server Log Messages** panel (Figure 16-2) contains a set of Action buttons that appear in the top of the list of the server log messages, as shown in Figure 16-1.

Table 16-1 Action buttons in the Server Log Messages panel

These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

To Insert a record, click on the  action button. The **Message Entry** panel is displayed as shown in Figure 16-3. This panel allows you to add a Log Message entry and corresponding properties as shown in Figure 16-3.

Figure 16-3 Server Log Messages panel-Message Entry panel

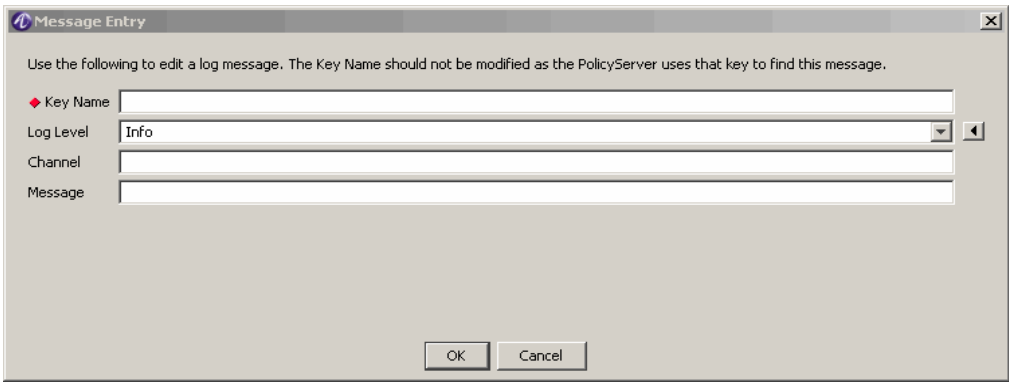


Table 16-2 explains each of these fields and the field descriptions that you will specify in this screen.

Table 16-2 The USSv2 StateServer Configuration-Add panel attributes

Field Name	Description
Key Name	Specifies the key name of the message.
Log Level	Specifies the Log Level in which the message will be logged.
Channel	The log channel to which the message will be logged.
Message	Specifies the contents of the message that will be logged.

To Edit a record, double click on a selected record or select a record and click on the  action button. The **Message Entry** panel is displayed as shown in Figure 16-3 with the existing values. This panel allows you to edit the contents of a Log Message entry and corresponding properties. Do not modify the Key name as the Policy Server uses this as a key to find this message.

Log Channels

About Log Channels

When 8950 AAA is first installed, all log messages are sent to the *policy.log* file. However, log messages can be directed to a wide range of other output destinations. Some destinations that can be used for log channels include, but are not limited to:

- Files
- Databases
- Syslog servers
- Network management Stations (SNMP)
- E-Mail

Each destination is known as a *log channel*. A log channel is uniquely named and is configured with specific properties. Names are usually chosen to provide a description of the channel. For example: LogToOracle, access-errors, NOC-Syslog-Server, etc.

Displaying Log Channel Information

Select **Log Channels** from the **Logging Tools** section on the Navigation pane. The *Log Channels* panel is displayed as shown in Figure 16-4.

8950 AAA uses Log Channels to output log messages. Log messages are typically errors, warnings, and information type messages. There are also other levels of messages used to track down problems such as debug level.

Using the Log Channels panel, you can specify the destinations for log messages. You can configure multiple output types by using the Wizard or the Insert button to add more than one channel. Once your channels are defined, use the LogRules panel to direct log messages to your channels.

Figure 16-4 Log Channels Panel

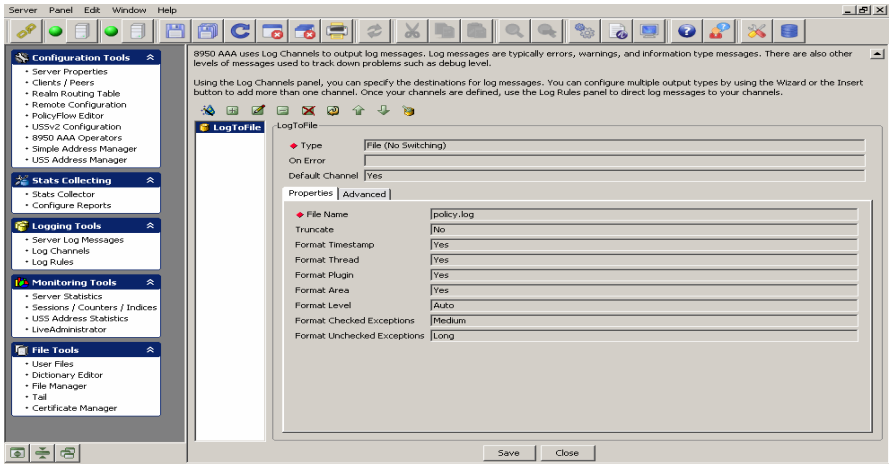


Figure 16-4 depicts the Log Channels panel showing information about a channel named *LogToFile*. When 8950 AAA is first installed, *LogToFile* is the only configured log channel. *LogToFile* sends messages to the file *policy.log*, which is in the 8950 AAA **run** directory.

On the left side of the Log Channels panel there is a list of log channel configurations. Select any item in the list to display its configuration characteristics. In Figure 16-4 there is only one item in the list.

The Log Channels panel contains a set of Action buttons that appear in the top of the list of log channel configurations, as shown in Figure 16-5.

Figure 16-5 Action buttons in the Log Channels panel

These action buttons allow you to perform the following actions:

- Insert Row Wizard
- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down
- Change the selected Channel to the Default Channel

You can perform any of the required actions using these action buttons.

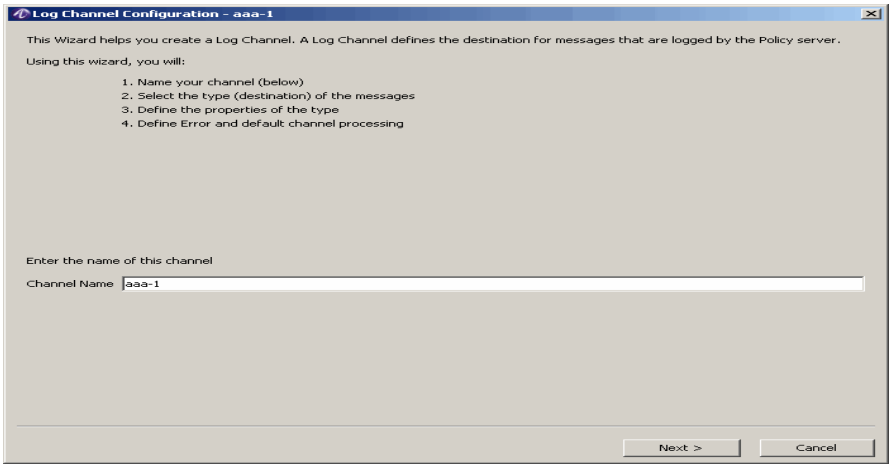
Configuring a Log Channel

The following procedure defines the steps of the built-in wizard that configures a log channel.

1. Select the  action button.

   Result: The Log Channel Configuration panel appears showing the first screen of the configuration panel, as shown in Figure 16-6. This screen prompts to enter the name of the Log Channel.

Figure 16-6 Log Channel Configuration Panel-Channel name

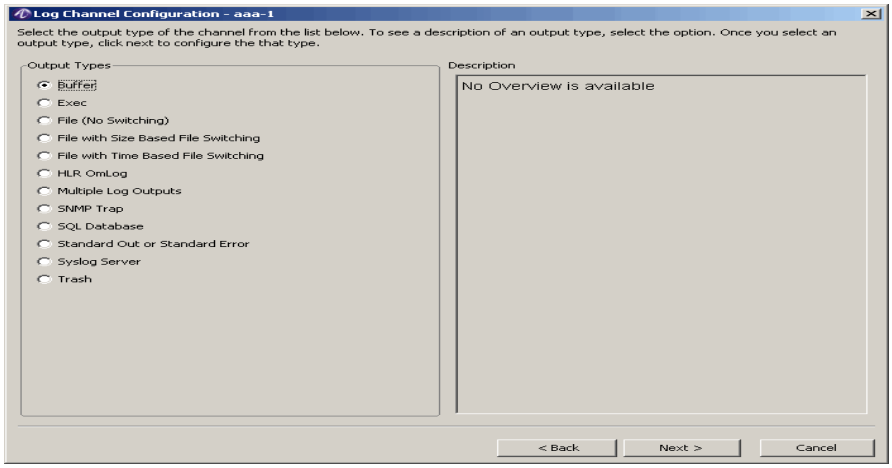


2. Enter a Log Channel name and click **Next**.

   Result: The Log Channel Configuration panel appears with a list of Output Types, as displayed in Figure 16-7.

   Important! Please refer to "Log Channel Configuration Panel Tabs" on page 14 for a description of each destination/output type that is listed.

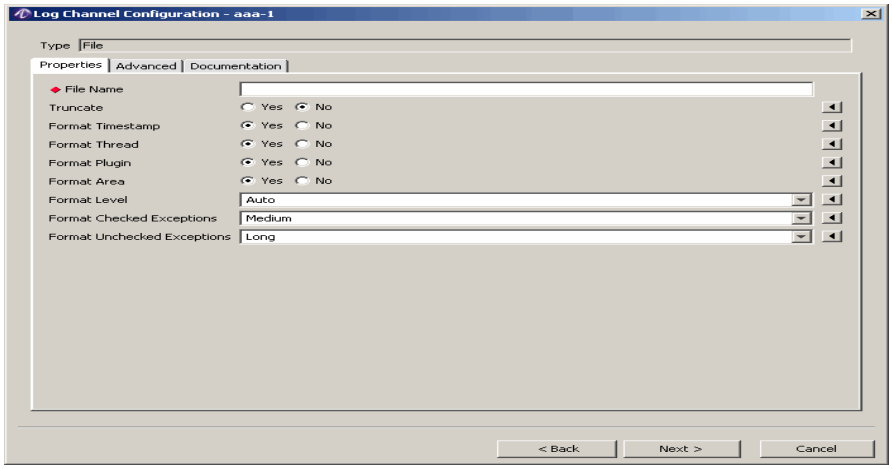
Figure 16-7 Log Channel Configuration Panel-Output Types



3. Select the required Output Type. The Description of the selected Output Type is displayed in the Description section of the panel. Click **Next** to define the properties of the channel.

   Result: The Log Channel Configuration Properties panel, that allows you to define the properties is displayed as shown in Figure 16-8. The properties in this screen will appear as per the Output types selected in Figure 16-7. The panel in Figure 16-8 is an example panel that appears when the Output Type File (No Switching) is selected.

Figure 16-8 Log Channel Configuration Panel-Properties tab



Common Log Channel Options

Each *Log Panel Configuration* panel contains a fixed section and a set of tabs that are dependent on the type of log channel being configured.

Every panel has a fixed section that contains four fields, as described in Table 16-3.

Table 16-3 Log Channel Configuration Panel-Properties tab

Field	Description
Name	The unique name for this channel.
Type	Pre-set with the selected destination type.
On-Error	Name of an alternate channel to use if an error is encountered while writing to this channel. 8950 AAA cannot determine if a Syslog server is responding. If syslog is your default output channel, you might wish define a redundant channel using a local file as the destination. See "Multiple Log Outputs" on page 22.
Default-Channel	If selected, then this channel is the *Default-Channel*. Only one channel may be designated at the *Default-Channel*. If you designate a channel as the *Default-Channel* it will automatically override any previous *Default-Channel* selection. If not selected, then the server uses the last selected default. The server uses this value when configuring Log Rules. It can be changed, but remember to check your Log Rules after changing. For more information, please see "Log Rules" on page 32.

Every panel contains three tabs that may be used to configure specific aspects of the log channel. They are the *Properties*, *Advanced*, and *Documentation* tabs. The use and contents of the tabs are dependent on the destination/output type of log channel selected.

The following options, in Table 16-4, are available for most but not all log channel options. They are discussed here for convenience and will not be repeated since they appear for each of the destination types described later in this section.

Table 16-4 Destination/Output Options

Field Name	Description
Format Timestamp	This checkbox controls whether 8950 AAA includes the timestamp in the logged message. For example, **`2008/01/21 13:45:30.870`** is the timestamp in the following message: **`2003/01/21 13:45:30.870 <nr.setup> 8950 AAA: Starting server initialization`**
Format Area	This checkbox controls whether 8950 AAA includes the log area in the log message. The log area is the part of the 8950 AAA server which logged the message. For example, **`<nr.setup>`** is the log area in the following message: **`2008/01/21 13:45:30.870 <nr.setup> 8950 AAA: Starting server initialization`**
Format Level	This pull-down provides three options for defining how the log level is formatted within a log message. The options are: • OFF - Never include the log level in the message. • AUTO - Include the log level in the log message only when the level is more severe than *Info*, that is, *Notice*, *Warning*, or *Error.* • ON - Always include the log level in the message.

Table 16-4 Destination/Output Options

Field Name	Description
Format Checked Exceptions	*Checked exception* - Error conditions that the 8950 AAA is able to check for and knows how to handle. These are normal operational errors that can occur in the 8950 AAA server. Four options are available to define the amount of information to include in a log message about a checked exception. The options are: • OFF - Never include the exception information in the log message. • SHORT - Include a brief description about the exception. • MEDIUM - Include a full description about the exception. • LONG - Include a full description about the exception with a JAVA *stacktrace.*
Format Unchecked Exceptions	*Unchecked exception* - Error conditions for which 8950 AAA does not have a pre-configured error handling routine defined. Four options are available to define the amount of information to include in a log message about an unchecked exception. The options are: • OFF - Never include the exception information in the log message. • SHORT - Include a brief description about the exception. • MEDIUM - Include a full description about the exception. • LONG - Include a full description about the exception with a JAVA *stacktrace.*

Table 16-4 Destination/Output Options

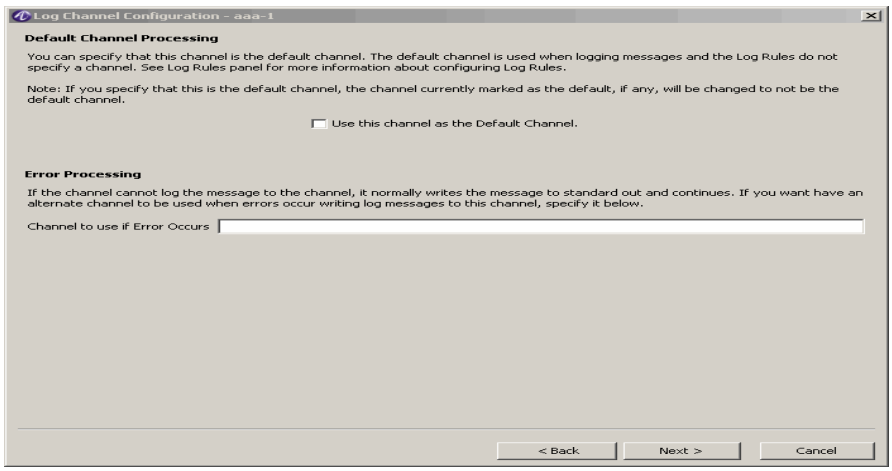
Field Name	Description
Char Set	Defines the character set the 8950 AAA Server uses when encoding the log message. Character sets that are available for selection: • 8859_1 • UTF8 • Others supported by Java as specified **Important!** For more information about character sets that support Java, please refer to the Web page found at the following URL: *http://java.sun.com/j2se/1.4.2/docs/api/java/nio/charset/Charset.html*

Important! Please refer to the section "Log Channel Configuration Panel Tabs" on page 14, for complete information on the tabs and field descriptions for each destination type.

4. Select the required properties and if required for your site, select the Advanced tabs (discussed below) and click **Next**.

   Result: The Log Channel Configuration Default and Error Channel Processing panel is displayed, as shown in Figure 16-9.

Figure 16-9 Log Channel Configuration Panel-Default and Error Channel Processing



5. You can choose to specify that this channel is the default channel. The default channel is used when logging messages and the Log Rules do not specify a channel.

Important! If you specify that this is the default channel, the channel currently marked as the default, if any, will be changed to not be the default channel.

If the channel cannot log the message to the channel, it normally writes the message to standard out and continues. If you want have an alternate channel to be used when errors occur writing log messages to this channel, specify it in the **Channel to use if Error Occurs** field.

6. After selecting the required channel(s), click **Next**.

   Result: A message appears indicating that channel configuration is complete.

7. Click **Back** to modify any values or **Finish** to return to the Log Channels panel.
8. Click **Save** to store your channel configurations to the server.

   Click **Close** to remove the panel.

   Log Channel additions and changes take affect the next time you start the 8950 AAA server.

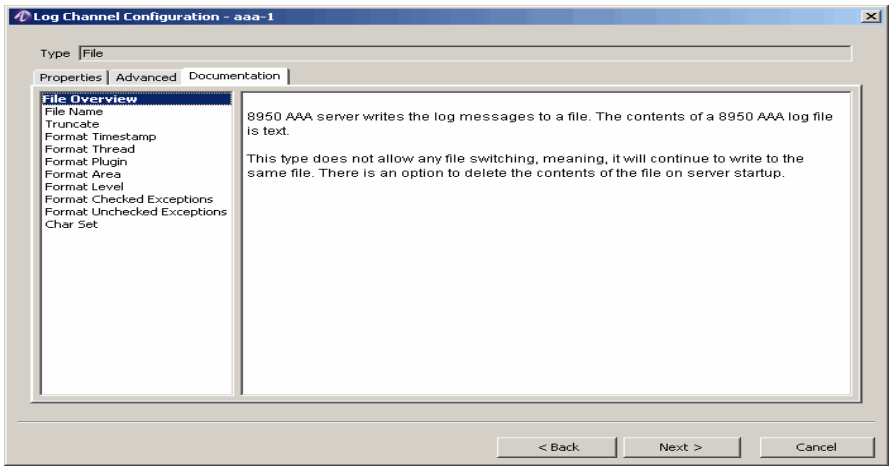
Log Channel Configuration Panel Tabs

About the Tabs in the Log Channel Configuration Panel

The three tabs within the variable section of the *Log Channel Configuration* panel are as follows:

- *Properties*–Basic information used for configuring this channel.
- *Advanced*–Additional fields that may be used to configure the channel.
- *Documentation*–Description of each property that appears in the Properties and Advanced tabs. The documentation tab provides a list of field names and a text area as shown in Figure 16-10. Select a field to display its description.

Figure 16-10 Log Channel Configuration Panel-Documentation Tab with File (No Switching) properties



The remainder of this section shows the Properties and Advanced tab for each log channel destination/output type with descriptions of each field.

Exec

The Exec destination executes an external process. Log data is written to the standard input of the external process. The data may include the following information: timestamp, area, log level, message text, or exception. A new process is started each time the log channel is invoked.

Figure 16-11 Exec-Properties Tab

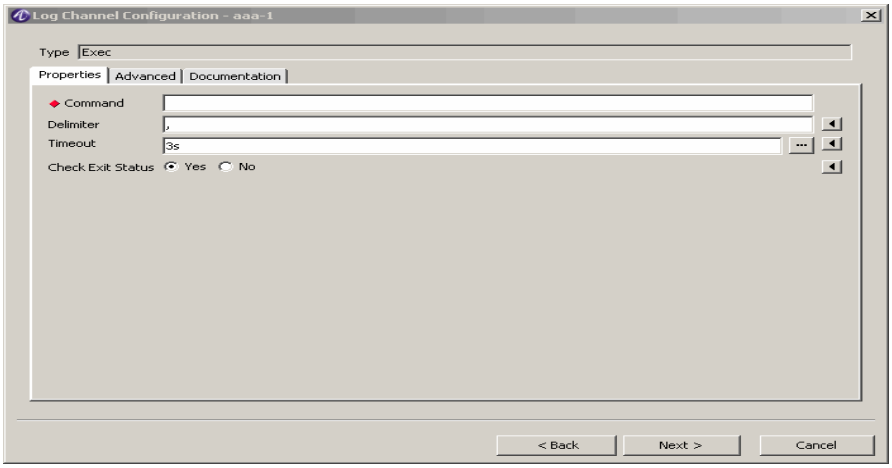


Table 16-5 explains each of these fields and the field descriptions that you will specify in this screen.

Table 16-5 Exec-Properties fields

Field Name	Description
Command	Command name, arguments, and directory paths necessary for command execution.
Delimiter	Separates data that is written to the standard input of the external process.
Timeout	Amount of time to wait for a process to complete execution **Important!** If the process does not complete within this time period, then a log message can be written to the log channel.

File (No Switching)

8950 AAA writes the log messages to a file. The contents of the log file is plain text. This type does not allow any file switching, which means that it will continue to write to the same file. There is an option to delete the contents of the file each time 8950 AAA is started. The properties tab for this destination type is shown in Figure 16-12.

Figure 16-12 File (No Switching)-Properties Tab

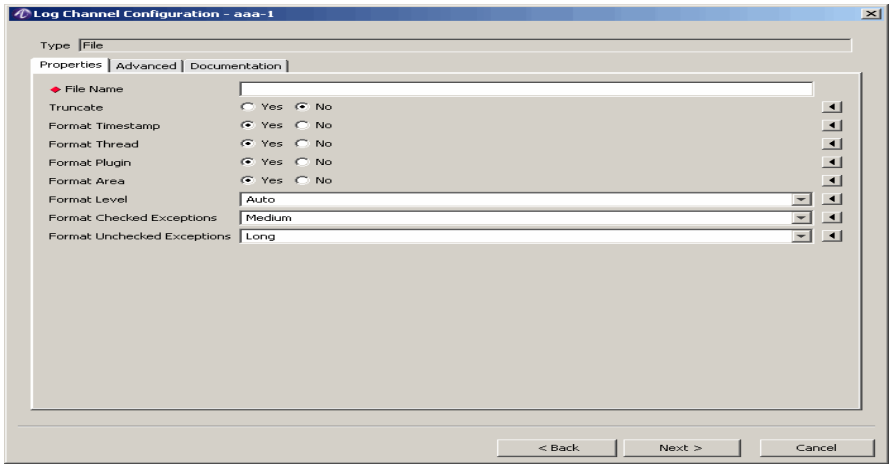


Table 16-12 explains some of the fields and the field descriptions that you will specify in this screen. Some of the fields are explained in .

Figure 16-13 File (No Switching)-Properties Fields

Field Name	Description
File Name	Name of the file to which this channel writes.
Truncate	If selected, delete contents of log file each time 8950 AAA restarts.

File with Size Based File Switching

The 8950 AAA writes the log messages to a file. 8950 AAA switches the log file it writes when a user specified file size is reached. The contents of the 8950 AAA log file is plain text. The properties tab for this destination type is shown in Figure 16-14.

Figure 16-14 File with Size Based File Switching-Properties Tab

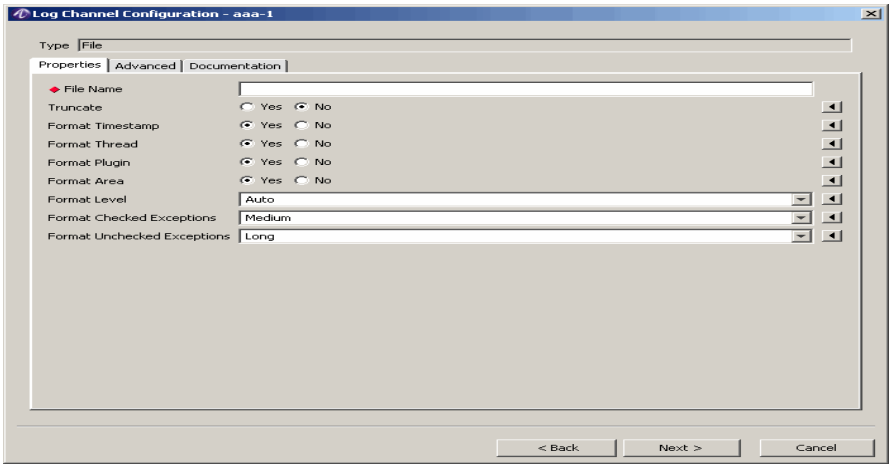


Table 16-6 explains the fields and the field descriptions that you will specify in this screen.

Table 16-6 File with Size Based File Switching-Properties tab Fields

Field Name	Description
Prefix	Specifies the prefix (beginning) portion of the log file name. **Important!** For more information please see *"Notes on the Naming of Time Based Files" on page 21*
Suffix	Specifies the suffix (ending) portion of the log file name. **Important!** For more information please see *"Notes on the Naming of Time Based Files" on page 21*
Size	Sets the size at which the log file is changed by the 8950 AAA server. **Example:** `20MB` where `20` is the size specified in this property and `MB` is specified in the *Unit* field.
Unit	Sets the unit by which *Size* is measured. Options are BYTES, KILOBYTES, MEGABYTES, and GIGABYTES

Notes on the Naming of Size Based Files

8950 AAA writes to a log file with the following name format:

<prefix> + active + <suffix>

The prefix and suffix components are specified by configuration settings. The name **active** is hard-coded by the 8950 AAA server. For example, if the prefix is **nr** and the suffix is **.log**:

The resulting log file name is: *nractive.log*

When a file is *switched*, also known as, *rolled-over*, the old, or saved, file name has the following format:

<prefix> + <timestamp> + <suffix>

The prefix and suffix portions are the same as above. The timestamp portion is hard-coded by the 8950 AAA server in format, `yyyyMMddHHmmssSSS`. Table 16-7 provides a breakdown of this format with examples.

Naming of Size based files–Format

Table 16-7 Naming of Size based files-Format

Timestamp Field	Meaning
yyyy	Four digit year, 2006.
MM	Two digit month, 12 for December.
dd	Two digit day in month, 03 for third day in month.
HH	Two digit hour in a 24-hour day.
mm	Two digit minutes in hour.
ss	Two digit seconds in minute.
SSS	Three digit milliseconds in second.

Using the example above, suppose the file *nractive.log* the currently open file is named.

If this file is switched January 1, 2006, at noon, then the name of the saved file will be *nr20060101120000000.log*.

File with Time Based File Switching

The 8950 AAA server writes the log messages to a file. 8950 AAA switches the log file it writes when a specified time interval is reached. Options are hourly, daily, weekly, monthly, or you can specify a custom time interval. The contents of a 8950 AAA log file is plain text. The properties tab for this destination type is shown in Figure 16-15.

Figure 16-15 File with Time Based File Switching-Properties Tab

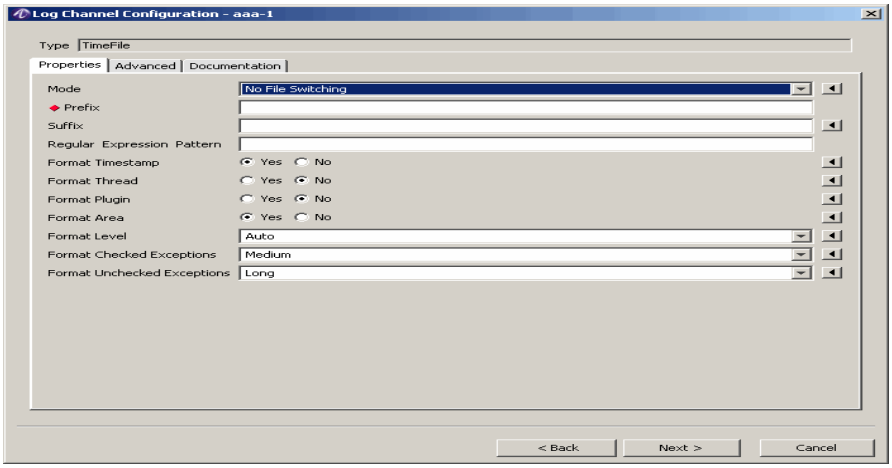


Table 16-8 explains the fields and the field descriptions that you will specify in this screen.

Table 16-8 File with Time Based File Switching-Properties tab Fields

Field Name	Description
Mode	Sets how often the log file is switched (the rolled-over interval). There are 5 options for this field: • HOURLY - The file is switched every hour. The timestamp portion is in format: **`yyyyMMddHH.`** • DAILY - The file is switched every day. The timestamp portion is in format: **`yyyyMMdd.`** • WEEKLY - The file is switched every week. The timestamp portion is in format: **`yyyyww.`** • MONTHLY - The file is switched every month. The timestamp portion is in format: **`yyyyMM.`** • CUSTOM - The rollover time and timestamp format is determined by the *Pattern* property.
Prefix	Specifies the prefix (beginning) portion of the log file name. **Important!** For more information please see *"Notes on the Naming of Time Based Files" on page 21*.

Table 16-8 File with Time Based File Switching-Properties tab Fields

Field Name	Description
Suffix	Specifies the suffix (ending) portion of the log file name. **Important!** For more information please see *"Notes on the Naming of Time Based Files" on page 21*.
Regular Expression Pattern	Specifies the timestamp pattern to use when CUSTOM is specified in the Mode property. Enter a pattern using a predefined time- or size-based format (see Table) that tells the server when to create a new file. When the specified pattern is exceeded, the server creates a new log file. The old file is given a name that follows the characteristics listed in *"Notes on the Naming of Time Based Files" on page 21*.

Notes on the Naming of Time Based Files

As described previously, 8950 AAA writes to a log file with the following name format:

<prefix> + <pattern> + <suffix>

where <**prefix**> and <**suffix**> are determined by the Prefix and Suffix field values set within the Properties tab and <**pattern**> is evaluated using the current time.

For example, if Prefix is **nr**, Suffix is **.log**, and the value of Mode is **MONTHLY** and the file is switched at the start of July, 2005, then the name of the file is *nr200507.log*.

If the value of Mode is **CUSTOM**, then the value of the Pattern field determines how often the log file is switched and the name of the saved file.

> **Important!** For a list of date and time expressions, including rules for using them, please refer to the Web page found at the following URL: *http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html.*

HLR OmLog

The HlrOmlog Channel cause the 8950 AAA server to inject log messages into the OMLOG subsystem. This channel is a thin wrapper on top of the HLR library function.

`com.lucent.packetin.output.Log.outputMessage.`

The properties tab for this destination/output type is shown in Figure 16-16.

Figure 16-16 HLR OmLog-Properties Tab

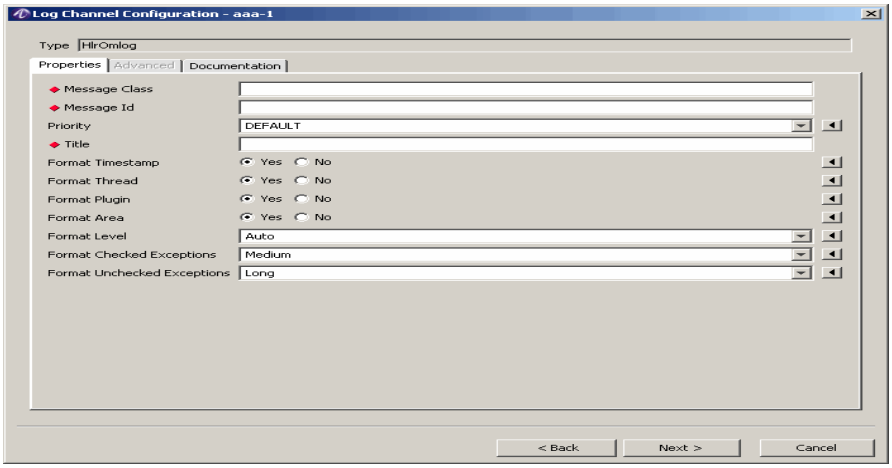


Table 16-9 explains the fields and the field descriptions that you will specify in this screen.

Table 16-9 HLROmlog-Properties tab Fields

Field Name	Description
Message Class	The Message Class can map to one or more files or communication links. Specifies where the message is to be printed.
Message ID	To uniquely identify the output message.
Priority	Appropriate alarm level to indicate the severity of the message.
Title	Appropriate title to which describes the process.

Multiple Log Outputs

The 8950 AAA server sends log messages to a list of channels for processing. This allows you to send a particular log message to more than one output. This can be used instead of using multiple channels with log rules. The log message is sent to all listed channels. The properties tab for this destination type is shown in Figure 16-17.

Figure 16-17 Multiple Log Outputs-Properties Tab

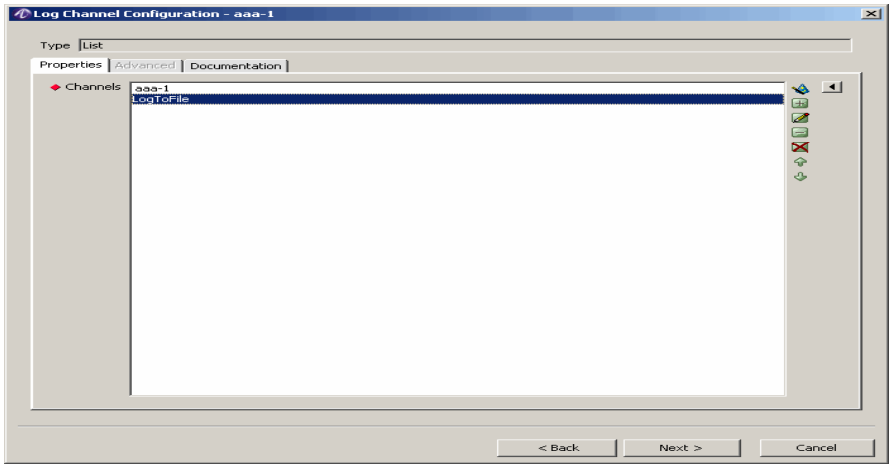


Table 16-10 explains the fields and the field descriptions that you will specify in this screen.

Table 16-10 Multiple Log Outputs-Properties tab fields

Field	Description
Channel	Specifies the list of channels to which 8950 AAA will write log messages. The 8950 AAA server sends the log message to each listed channel for processing. The listed channels must have been previously defined. Each channel controls the formatting of the message.

SNMP Trap

The SNMP Trap destination type allows 8950 AAA to write log messages to an SNMP version 1 management system. The messages are sent as SNMP Traps. The Properties tab is shown in Figure 16-18. The Advanced tab is shown in Figure 16-19.

Figure 16-18 SNMP Trap-Properties Tab

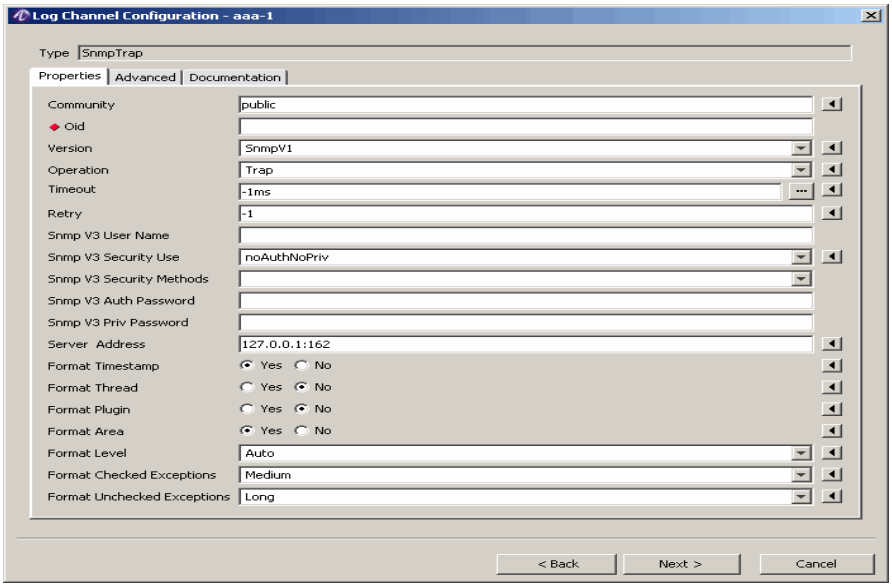


Table 16-11 explains the fields and the field descriptions that you will specify in this screen.

Table 16-11 SNMP Trap-Properties tab fields

Field Name	Description
Community	Sets the SNMP v.1 community string.
OID	Sets the SNMP object identifier.
Version	The SNMP version to be used.
Operation	The operation to be performed.
Timeout	Amount of time to wait for the response, after which you can retry.
Retry	The number of time you can retry.
SNMP V3 User Name	The SNMP V3 user name.
SNMP V3 Security Use	This is a SNMP V3 security credential (to be retrieved from the SNMP V3 administrator.)
SNMP V3 Security Methods	This is a SNMP V3 security credential (to be retrieved from the SNMP V3 administrator.)
SNMP V3 Auth Password	This is a SNMP V3 security credential (to be retrieved from the SNMP V3 administrator.)
SNMP V3 Priv Password	This is a SNMP V3 security credential (to be retrieved from the SNMP V3 administrator.)

Table 16-11 SNMP Trap-Properties tab fields

Field Name	Description
Server Address	Defines the host/IP of the SNMP management system. The Server Address is in format host:port. Example: `127.0.0.1:162`

Figure 16-19 SNMP Trap-Advanced Tab

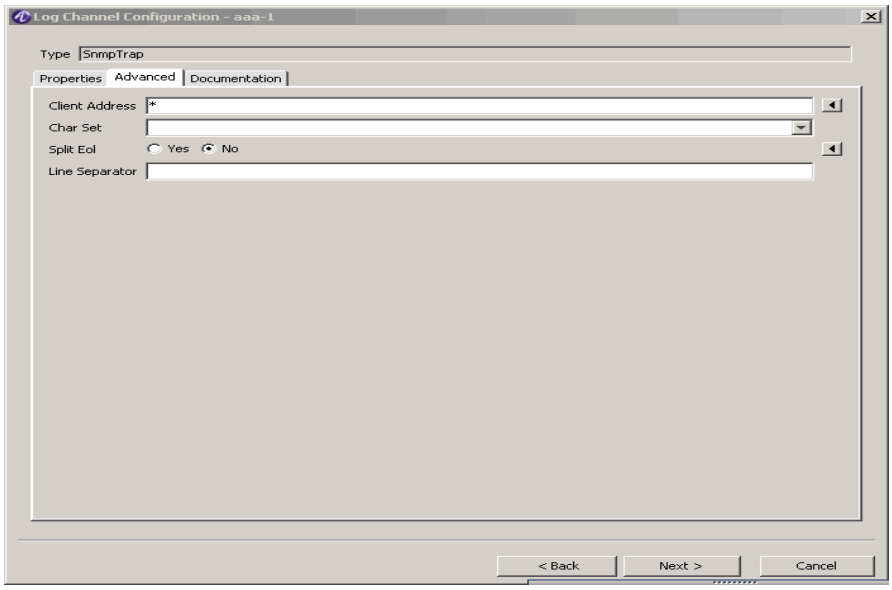


Table 16-12 explains the fields and the field descriptions that you will specify in this screen.

Table 16-12 SNMP Trap-Advanced tab fields

Field	Description
Client Address	Sets the source IP address and/or source port number of the SNMP trap.
Char Set	The character set to be used for the log messages.
Split EOL	To split the messages based on line separator.
Line Separator	The character to be used as the line separator.

Important! The SNMP administrator should fill in the values for the attributes mentioned in Table 16-12.

SQL Database

The Database channel writes log messages to a SQL compliant database. Each 8950 AAA log message is represented by a row (record) in the database table. Every log message in 8950 AAA contains the following pieces: Timestamp, Thread, Area, Level, Message, and a Java Stacktrace. Each of the pieces can be saved independently of each other to a database.

> **Important!** The use of the Database channel and the following discussion assumes you are familiar with SQL and general database issues, have an SQL compliant database running on an assessable system, and have a JDBC driver for that database installed.

The properties tab for this destination/output type is shown in Figure 16-20.

Figure 16-20 SQL Database-Properties Tab

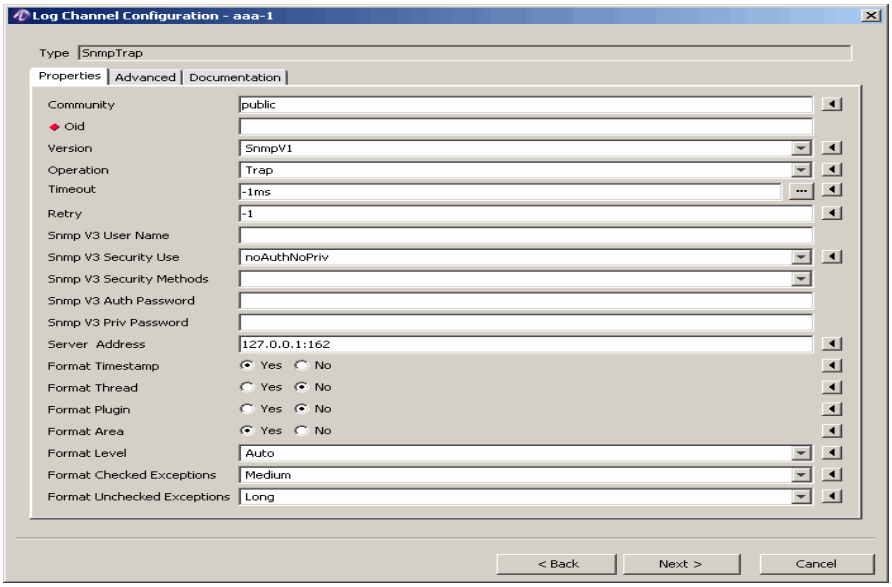


Table 16-13 explains the fields and the field descriptions that you will specify in this screen.

Table 16-13 SQL Database-Properties tab fields

Field Name	Description
Driver	Database driver. This is a required field.
URL	Uniform Resource Locator (URL) of the database. This is a required field.

Table 16-13 SQL Database-Properties tab fields

Field Name	Description
USER (Administrator User Name)	Sets the login used to connect to the database server with permission to write to the log table. This is a required field.
Password	Sets the password for the Administrator User Name.
Table	Sets the name of the database table used to store log messages. The default is *LOG*.
Sequence Column	Sequence value typically not used unless identity-type columns are used in your database. This is an optional field; the data type is *long*.
Timestamp Column	Column time that the log action occurred. This is an optional field; the data type is *timestamp*.
Thread Column	Specifies the name of the column in the database table, to store the name of the Java thread of the log message.
Plugin Column	Specifies the name of the column in the database table, to store the name of plugin that generate the log message.
Area Column	Section of code associated with the log action. This is an optional field; the data type is *varchar*.
Level Column	Number associated with the log level. This is an optional field; the data type is *integer*.
Level Name Column	Name associated with the log level. This is an optional field; the data type is *varchar*.
Message Column	Formatted text of the message. This is an optional field; the data type is *varchar*.

Standard Output or Standard Error

When logging to Standard Out or Standard Error, 8950 AAA sends log messages to the system file descriptor for standard_output (stdout) or standard_error (stderr). If stdout or stderr is not redirected, messages will appear in the same command window in which 8950 AAA was started. The properties tab for this destination type is shown in Figure 16-21.

Figure 16-21 Standard Output or Standard Error-Properties Tab

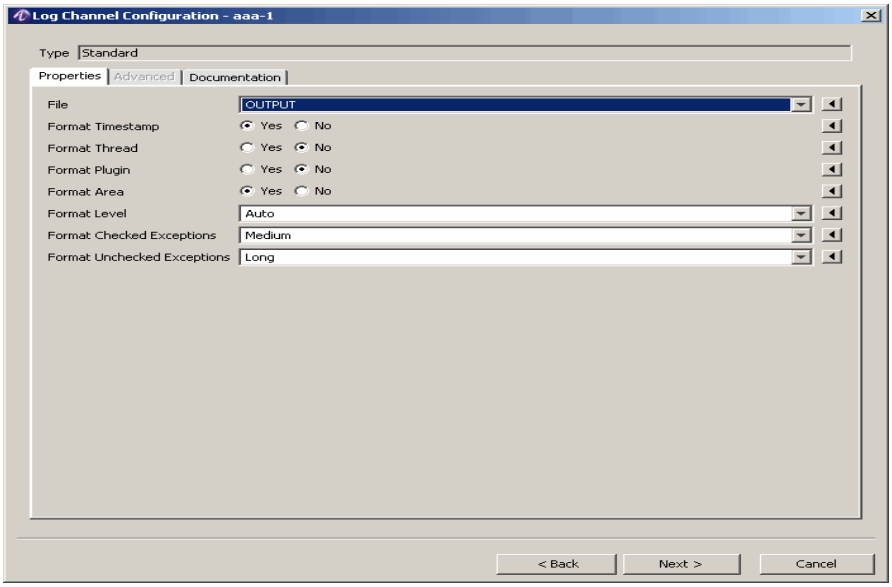


Table 16-14 explains the fields and the field descriptions that you will specify in this screen.

Table 16-14 Standard Output or Standard Error-Properties tab fields

Field Name	Description
File	Defines the file descriptor to which 8950 AAA will write the log messages. There are 2 options for this field: • OUTPUT - Messages are written to *Standard Out.* • ERROR - Messages are written to *Standard Error.*

Syslog Server

This log channel destination type sends log messages to a Syslog server. Because of the way the syslog protocol operates, 8950 AAA cannot determine if the messages are actually received by the syslog server, or if errors occur while the syslog server is processing the log messages. Because of this, the log channel defined in the *On-Error* will only be used for errors that occur within the 8950 AAA server. The properties and advanced tabs are displayed in Figure 16-22 and Figure 16-23, respectively.

Figure 16-22 Syslog Server-Properties Tab

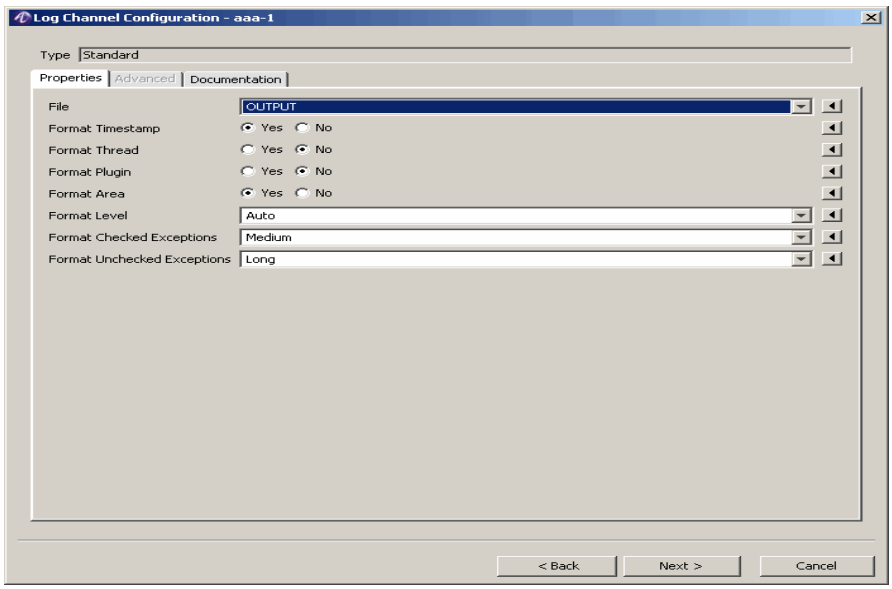


Table 16-15 explains the fields and the field descriptions that you will specify in this screen.

Table 16-15 SysLog Server-Properties tab fields

Field Name	Description
Server Address	Defines the host/IP of the syslog server. The Server Address is in format host:port. Example: `192.168.1.4:514` The default is *127.0.0.1:514* (A Syslog server running on the local host.)
Facility	Defines the part of the system generating the message. Example: `kern` The default is *auth*.
Priority	Defines the priority to change all messages logged by 8950 AAA. Example: `alert` The default is *map*, which converts 8950 AAA log levels to Syslog severity levels.

Table 16-15 SysLog Server-Properties tab fields

Field Name	Description
Cutoff	Defines the maximum 8950 AAA log level to send to the syslog server. Example: `NOTICE` Only 8950 AAA messages logged at levels NOTICE, WARNING and ERROR and higher will be sent to the Syslog server. The default is *INFO*.
Process Name	Defines the application name of the messages sent to the syslog server. Example: `8950 AAA` The default is `NR`.
Format Host Name	Determines whether the hostname, in which the 8950 AAA server is running, is included in the message sent to the Syslog server. The default is *unchecked* (the hostname is not included).

Figure 16-23 Syslog Server-Advanced Tab

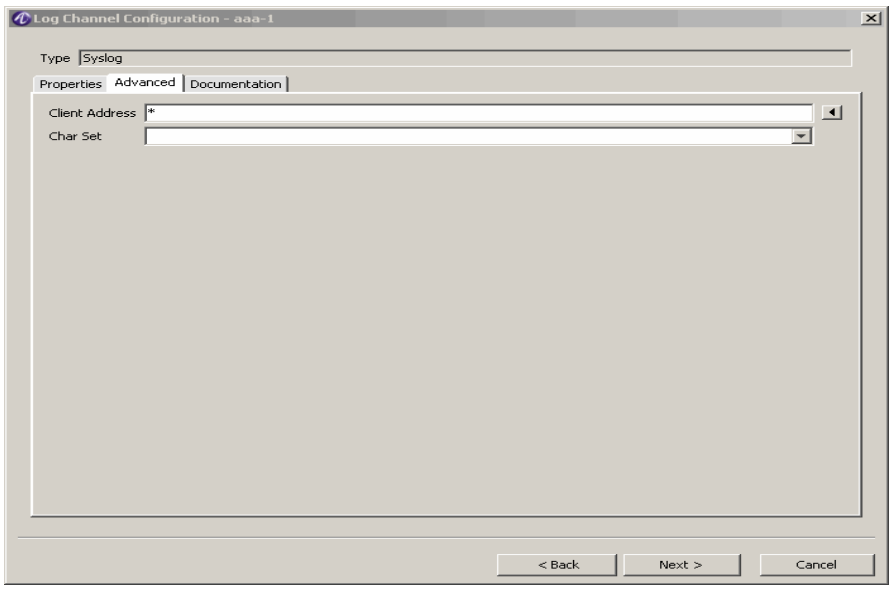


Table 16-16 explains the fields and the field descriptions that you will specify in this screen.

Table 16-16 SysLog Server-Advanced tab fields

Field	Description
Client Address	Sets the source IP address and/or source port number of the Syslog message that is sent to the server
Char Set	The character set to use to be used for the log message.

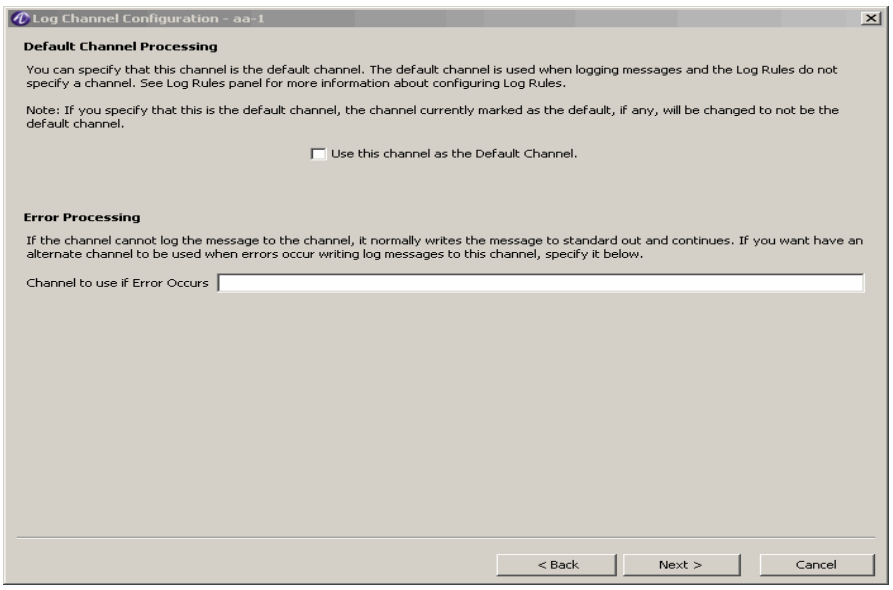
Trash

The Trash Channel causes the 8950 AAA server to silently discard the log message. The *Trash* destination is typically used for excluding certain log output by temporarily dropping output that results from a *Log Rule*.

For more information, please refer to "Log Rules" on page 32.

The properties tab for this destination type is shown in Figure 16-24.

Figure 16-24 Thrash-Properties Tab



Log Rules

About Log Rules

8950 AAA logging is divided into two separate functional parts:

1. Log message generation

   The following three factors determine when a log message is created:

   a. Log Area

      The Log Area is a *limited wildcard pattern* (see note below) used to indicate a program area. 8950 AAA is divided into several program *areas.* Each 8950 AAA program area performs a specific function. For example, accessing external files, request queue management, request decoding, command execution, plug-in execution, etc. Each program area contains software instructions that determine when a log message should be created.

   b. RADIUS Request Expression

      The RADIUS Request Expression is a limited wildcard pattern used for filtering messages. It is optional.

c. Log Level

The Log Level is determined by the conditions that are associated with it.

The decision to log a message depends on the Log Area, the RADIUS request expression (if used), and the Log Level. If the current log level and RADIUS request expression match the requirements of the log code in the current area, then a message is generated.

2. Log message disposition

Once a message is generated, it must be sent to a destination or Log Channel, as described starting on this item. *Log Rules* determine the Log Channel that is the destination of the log message.

Important! The asterisk (*) provides limited wildcard matching capabilities for Log Area and RADIUS Request Expressions. It matches textual data when it is used either at the beginning or at the end of an expression. For example,
*abc is valid
abc* is valid
abc is invalid
ab*c is invalid

Log Rules - Definition and Use

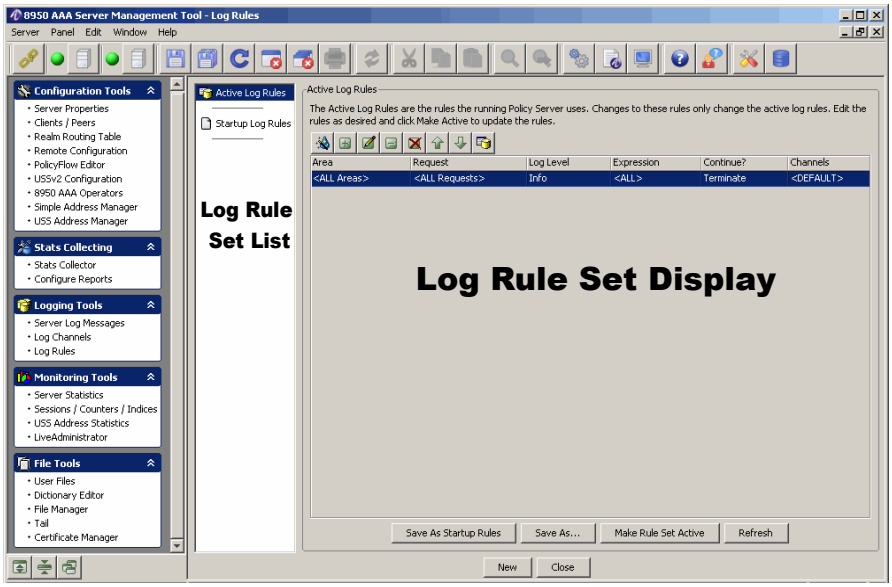
In 8950 AAA, *Log Rules* define the conditions under which messages will be logged and the Log Channel or Channels to which the messages will be sent.

To display the Log Rules panel, select **Log Rules** from the Navigation Area, as shown in Figure 16-25.

Figure 16-25 Navigation Pane-Log Rules

Figure 16-26 depicts the Log Rules panel, with its two sections labeled.

Figure 16-26 Log Rules Panel



There are two sections within the Log Rules Panel:

- *Log Rule Set List*:
  - Contains the names of available *Log Rule* sets
  - You may select a *Log Rule* set from this list by clicking on it
  - The list is divided into three sections:
  - Active Log Rules
    Log Rules currently in effect in the running 8950 AAA server. This choice cannot be selected when the *8950 AAA* server is not running.
  - Startup Log Rules
    A set of *Log Rules* that are loaded automatically whenever 8950 AAA starts.
  - Other Log Rule set files
    Other sets of *Log Rules* that you may optionally create.

  Important! Log rule sets you create are saved in the 8950 AAA run directory with the filename extension ".lr".
- *Log Rule Set Display*
  - Shows the log rule from the Log Rule set that is highlighted in the *Log Rule Set List*
  - The title of this panel section is the name of the selected *Log Rule Set*
  - Figure 16-26 shows the title *Active Log Rules.*

Parts of a Log Rule

Every log rule has 6 parts as described in Table 16-17.

Table 16-17 Parts of a Log Rule

Log Rule Field	Description
Area	8950 AAA server program area for which this log rule is used.
Request	Indicates whether this log rule affects all RADIUS requests or only RADIUS requests that match a defined pattern.
Log Level	Starting log level for which this log rule is used.
Expression	If the Request field indicates pattern-matching, then this is a regular expression that is used for matching against the formatted log message.
Continue?	Indicates whether to use the next active log rule after this one is executed, or not.
Channels	Indicates one or more log channels to which messages logged by this rule are sent. If this field is not set to a value, then it uses the default channel.

Creating a New Log Rule

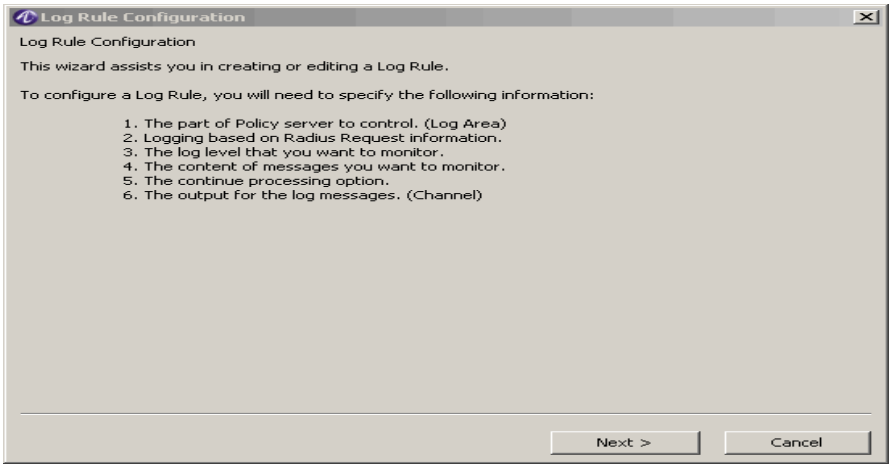
Use the following procedure to define a log rule. The new *Log Rule* you create will be created in the *Log Rule* set currently highlighted in the *Log Rule Set List*.

The following procedure defines the steps of the built-in wizard that configures a new log rule.

3. Select the  action button.

   Result: The Log Rule Configuration Wizard appears showing the first screen of the configuration panel, as shown in Figure 16-27. This screen assists you in creating or editing a Log Rule.

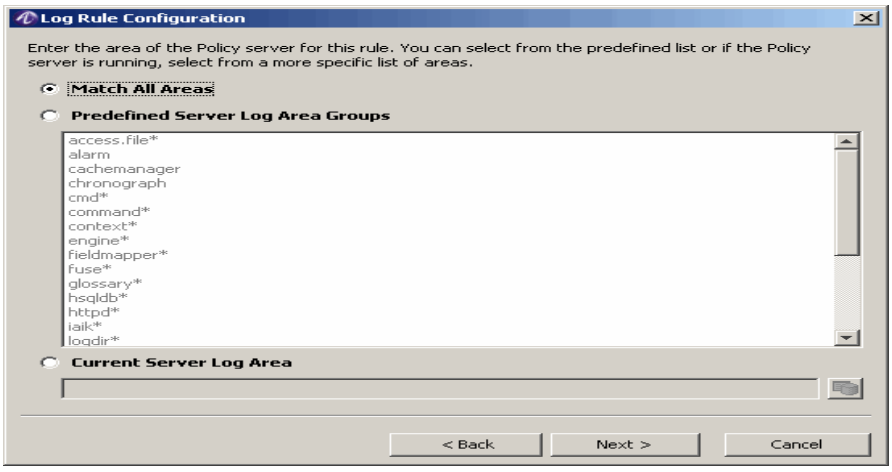
Figure 16-27 Log Rule Configuration Wizard



4. Click **Next**.

   Result: The first Log Rule Configuration panel is displayed as shown in Figure 16-28.

Figure 16-28 Log Rule Configuration Wizard-Log Area



5. In this step you will select the 8950 AAA *Log Area* to which this rule will apply.

   Pick one of the following three options:

   - *Match All Areas* - If selected, this rule will apply in all *8950 AAA Log Areas*.
   - *Predefined Server Log Area Groups* - Program areas that are present regardless of the configuration and PolicyFlow and collections of related. Here are a few examples:

   – *nr.setup* – system startup

   – *plugin.** – the execution of any 8950 AAA plug-in.

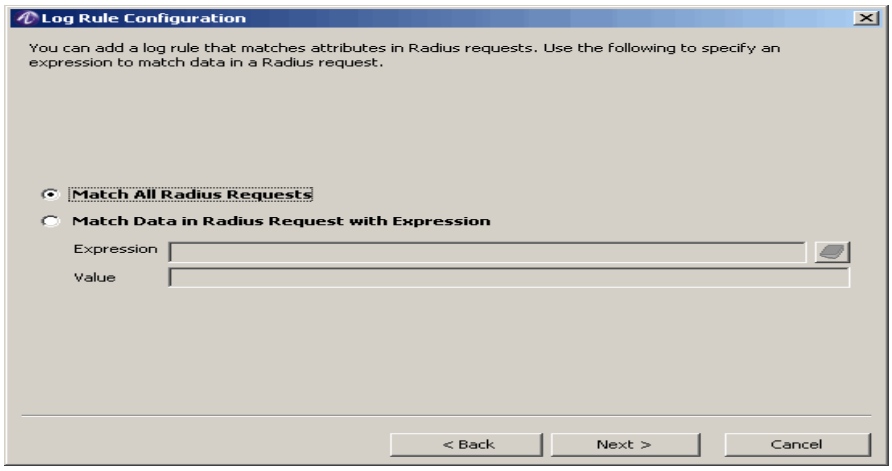
   – *engine.** – all areas that work with managing the flow of a request through the PolicyFlow or PolicyAssistant.

- *Current Server Log Area* - A specific area of the running 8950 AAA server. These areas include one area for each plug-in in the PolicyFlow program, one for each engine listener, etc. You may click  to see a list of the currently available *Log Areas*. This option is available only when the *8950 AAA* server is running.

6. When done, click **Next**.

   Result: The Matching Rule panel appears as shown in Figure 16-29.

Figure 16-29 Log Rule Configuration Wizard-Matching Rule



7. In this step you may define a matching rule to test the value of 8950 AAA PolicyFlow variables.
   - *Match All Radius Requests* - All RADIUS requests will be considered for logging
   - *Match Data in Radius with Expression* - Only those RADIUS requests that match the limited wildcard expression will be considered for logging. Further, logging will only occur at those times when the expression is valid. For example, if a 8950 AAA variable matched in an expression changes value during the processing so that it no longer matches the expression, the logging will stop.

   – Enter an expression - Expressions are matched against PolicyFlow variables, such as,

     ${request.User-Name}

   – Enter the value that the expression must match

     A possible value for the expression noted above might be

     ```
     *@alcatel-lucent.com
     ```

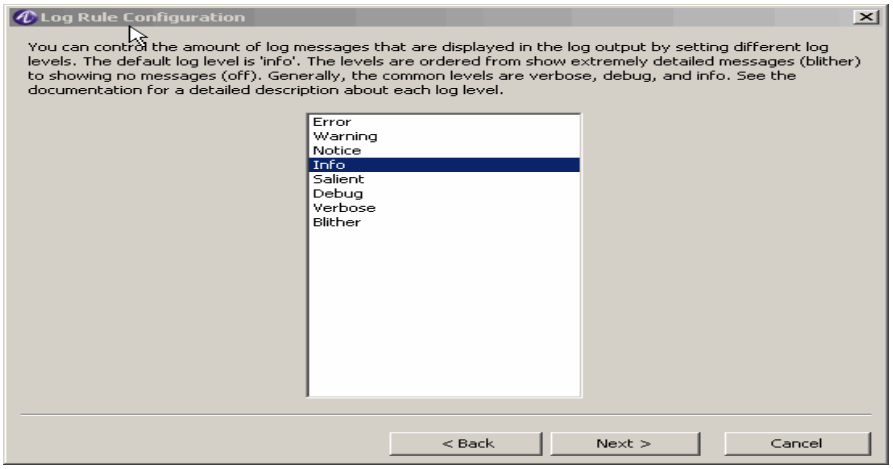
Important! It is possible to match against more than one value. For example, the expression: ${request.User-Name}-${request.NAS-IP-Address} might be matched against the value “rdp-10.0.1.2” This expression would only match requests where the User-Name was “rdp” and the request originated from a client with an address of *10.0.1.2*.

8. When done, click **Next**.

   Result: The next panel of the Log Rule Configuration Wizard appears for setting the value level field of the log rule that is being defined, as displayed in Figure 16-30.

9. In this step you will set the *Log Level* that must be matched in this *Log Rule*.

Figure 16-30 Log Rule Configuration Wizard-Log Level



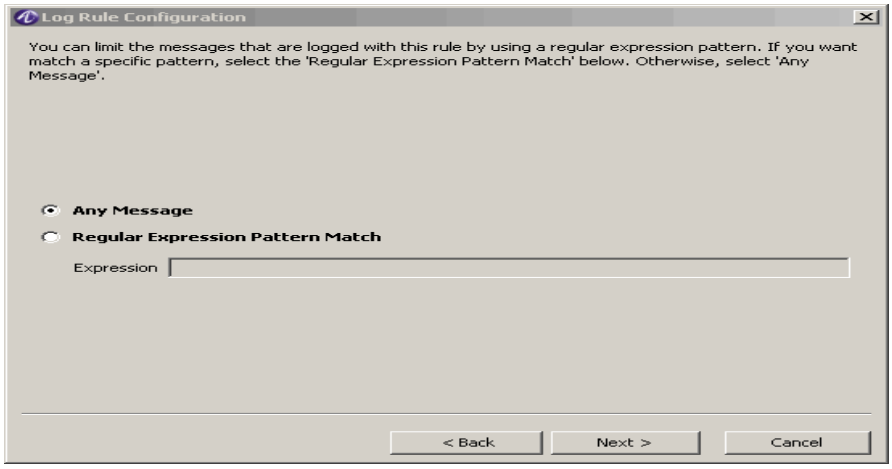
Select a log level that will determine messages to be sent.Only messages logged at this, or a more severe level, will be output.

Important! Log Level Blither is the least severe Log Level, and prints out large amounts of information about very arcane aspects of the server operation. Log Level ERROR is the most severe Log Level and only prints out the most critical messages.

10. When done, click **Next**.

    Result: The next panel of the Log Rule Configuration Wizard appears for controlling messages, as shown in Figure 16-31.

Figure 16-31 Log Rule Configuration Wizard-Pattern Match



11. In this step you may define any log message patterns that must be matched. These patterns are created using standard *Regular Expression* syntax. The Regular Expression is matched against the text content of the log message. This is different from the Expression entered in step 3 which was matched against 8950 AAA PolicyFlow variables.

    Select one of the two available options:

    - Any Message - indicates that there is no restriction on the log message
    - Regular Expression Pattern Match - indicates that only messages that contain the entered pattern are logged.

    Important! The following examples show Regular Expressions:

    ```
    /San Francisco/
    -abc/def-i
    ```

    The first example uses slashes (/) to delimit the character string. An exact match of the character string must occur for a message to be logged.

    The second example uses hyphens (-) to delimit the character string because the slash is a valid character of the string. It also uses a pattern match modifier (i) to indicate that case is ignored. The case does not have to match for a message to be logged. Pattern match modifiers are listed as follows:

    i - ignore case

    m - multi-line

    s - single line

    x - extended syntax

    Important! Use Regular Expression syntax per Rule 5 Regular Expressions.

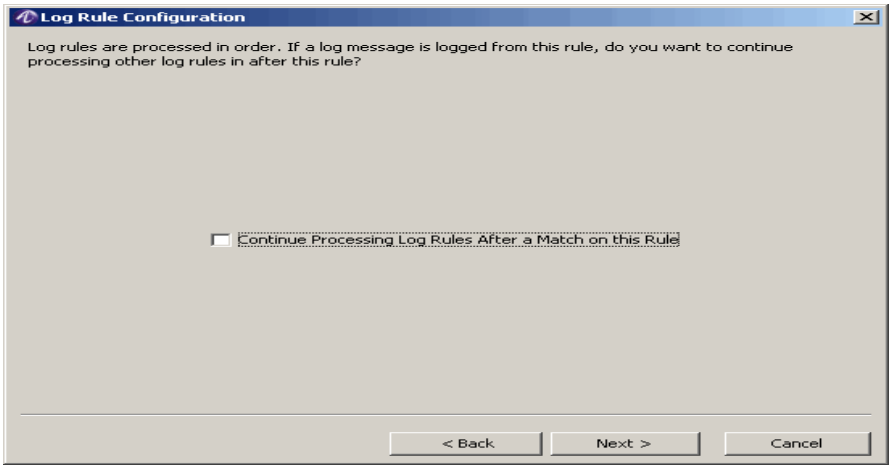
    For further reading, please refer to:

Mastering Regular Expressions (2nd ed.). Jeffrey E. F. Friedl. O'Reilly & Associates, Inc., July, 2002. (ISBN 0-59600-289-0)

12. When done, click **Next**.

    Result: The next panel of the Log Rule Configuration Wizard appears for executing log rules, as shown in Figure 16-32.

Figure 16-32 Log Rule Configuration Wizard-Continue Processing



13. In this step, you define what 8950 AAA will do following execution of this Log Rule.

    By default, 8950 AAA examines the Log Rules in the Active Rule Set starting with the first rule and works down through the last rule until it finds a Log Rule that matches all of its criteria (Log Area, Expressions, Log Level, etc.) After a matching rule has been executed, and the log messages have been sent to the appropriate Log Channels, no additional Log Rules are evaluated.

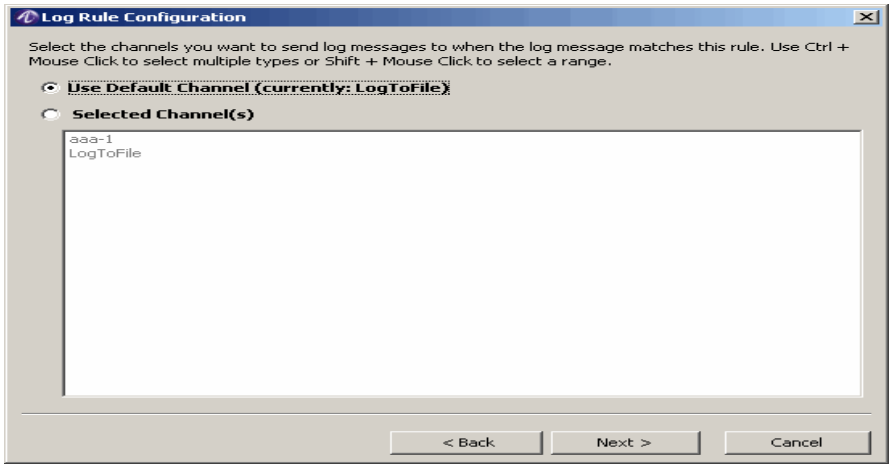
    For example if the first Log Rule matches all requests for all Log Areas with no log message expressions, then it is always executed and any additional Log Rules are never evaluated.

    This default behavior can be changed by selecting the Continue Processing Log Rules After a Match on this Rule option. If this option is selected, then, 8950 AAA will evaluate the next Active Log Rule after this Log Rule is executed.

14. When done, click **Next**.

    Result: The next panel of the Log Rule Configuration Wizard appears for assigning one or more Log Channels for this rule, as shown in Figure 16-33.

Figure 16-33 Log Rule Configuration Wizard-Message Destination



15. In this final step you will select the *Log Channel* or Log Channels to which log messages should be sent.

    One or more items may be selected from the list as follows:

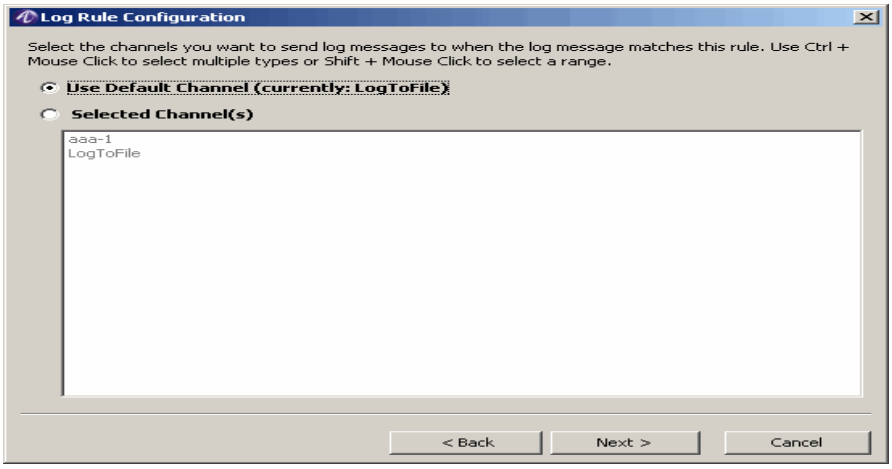
Table 16-18 Log Channel Selection

To select one Log Channel	Click the Log Channel name
To select a range of Log Channels	While holding the SHIFT, select the desired range
To select more than one Log Channels, not in a range	While holding the CTRL key, select the desired Log Channel names

16. When done, click **Next**.

    Result: The Log Rule Configuration Summary panel appears as shown in Figure 16-34.

Figure 16-34 Log Rule Configuration Wizard-Completion

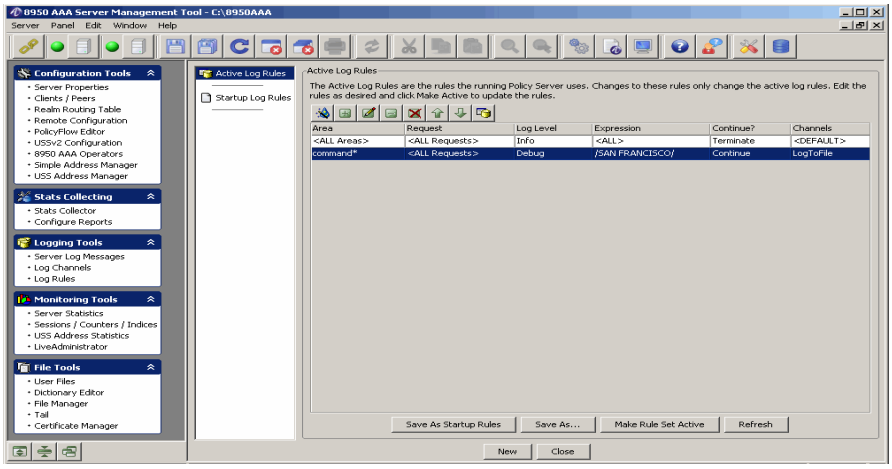


17. This step provides a way to verify the Log Rule information.

    Verify the data and click < **Back** to modify any of the previous screens or click **Finish** if you are complete.

    Result: The Log Rules panel appears with the new Log Rule listed in the Log Rule Set Display, as shown in the example in Figure 16-35.

Figure 16-35 Log Rule Configuration-New Log Rule



Reordering Log Rules

Use the reorder buttons to arrange the order of the Log Rules. Order is very important. Log Rules are evaluated from top to bottom until a match is found. Evaluation stops after a match is found unless the *Continue Processing Log Rules After a Match on this Rule* option was selected for a rule.

The reorder buttons, the up and down arrow key buttons, are also on the top of the panel with the other action buttons.

Follow these steps to move a log rule to a different position within the Active Log Rules list:

1. Select the log rule entry that is to be moved
2. Click the up or down arrow button enough times to move the log rule entry to the desired location.

Activating Log Rules

From the Log Rules Panel, perform the following steps to activate Log Rules:

- Click the **Save As Startup Rules** button to preserve the current set of Log Rules.
- Click the **Save As...** button to write the current set of Log Rules to a new file.
- Click the **Make Rule Set Active** button to activate the present set of rules.
- Click the **Refresh** button to update the Log Rules Panel.

Important! When Log Rules from a Log Rule set are made active, all of the rules in the set are made active. It is not possible to only activate some rules in a set. If you have Log Rules you frequently use alone for special purposes you might consider placing them in a Log Rule Set by themselves.

END OF STEPS

Part IV: Monitoring Tools Navigation Pane

Overview

Purpose

This part consolidates the chapters related to Monitoring Tools in the SMT Navigation pane.

Contents

This part includes the following chapters.

17 Server Statistics

Overview

Purpose

This section discusses the tools that are available for monitoring 8950 AAA activity. Such tools help to monitor RADIUS traffic levels and diagnose problems.

The following topics are included in this chapter:

Monitoring Server Statistics

About Monitoring Server Statistics

There are two panels that are used for viewing activity of the 8950 AAA Server. They are located under the SMT Navigation Area, under Monitoring Tools. They are:

- The Server Statistics Panel
- The Ports / Counters Panel

The following sections describe the capabilities of both panels.

> **Important!** The Live Administrator is another tool used for monitoring and managing 8950 AAA while it is running.

Server Statistics Panel

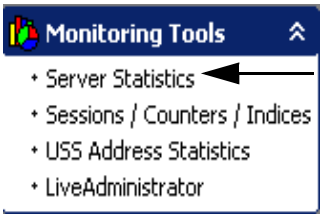
About Server Statistics Panel

The Server Statistics panel provides the ability to monitor the following aspects of 8950 AAA server operations:

- **Requests to and responses from** the 8950 AAA server
- **Requests and responses to** 8950 AAA from other servers
- State Server (USS) activity
- PolicyFlow program execution

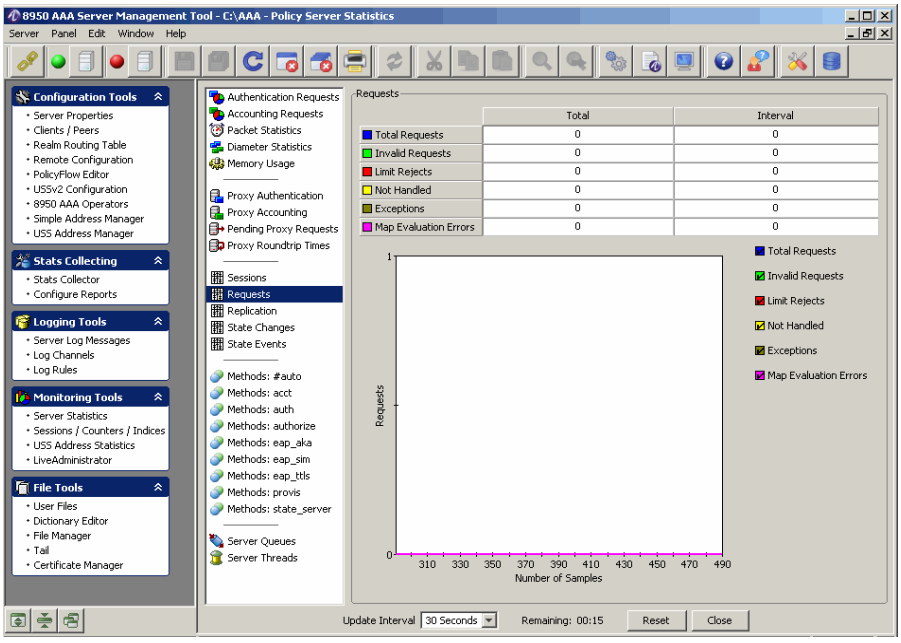
To display the Server Statistics panel, use the SMT Navigation Pane to select **Server Statistics** under Monitoring Tools, as shown in Figure 17-1.

Figure 17-1 Navigation Pane-Server Statistics



The Server Statistics Panel appears as shown in Figure 17-2.

Figure 17-2 Server Statistics Panel



This panel contains two sections as follows:

- The left section contains a list of program functions about which monitoring capabilities are available.
- The right section displays information about the selected item.

Table 17-1 lists each screen name and the information that it monitors.

Table 17-1 Server Statistics Panel-Screen Names and information

Screen Name	Monitored Information
"Authentication Requests" on page 4	Counts / percentages based on request disposition.
"Accounting Requests" on page 6	Counts / percentages based on request disposition.
"Packet Statistics" on page 8	Total number of radius packets processed.
"Diameter Statistics" on page 9	Total number of diameter packets processed.
"Memory Usage" on page 10	Amount of memory used by 8950 AAA and the Java Virtual Machine (JVM).
"Proxy Authentication" on page 12	Counts / percentages based on request status for Access-Requests forwarded to other servers.
"Proxy Accounting" on page 13	Counts / percentages based on request status for Accounting-Requests forwarded to other servers.
"Pending Proxy Requests" on page 15	Proxy requests waiting for a response from other servers.
"Proxy Roundtrip Times" on page 16	Time for a proxy request to return.
"Sessions" on page 18	Number of active sessions present on the server.
"Requests" on page 19	Number of authentication or accounting requests sent to the server.
"Replication" on page 20	Replication of the sessions between two servers.
"State Changes" on page 22	Monitoring the transition of states.
"State Events" on page 22	Monitoring the events which trigger a state change.
"Methods: #auto" on page 26	Automatically executed Methods.

Table 17-1 Server Statistics Panel-Screen Names and information

Screen Name	Monitored Information
"Methods: aaa" on page 26	Execution of Methods under the aaa policy flow file.
"Server Queues" on page 27	Request queue size, maximum value, and high water mark.
"Server Threads" on page 27 *	Status of currently running threads.

Screens that Monitor RADIUS Requests Sent to the 8950 AAA Server

This section describes the following four screens:

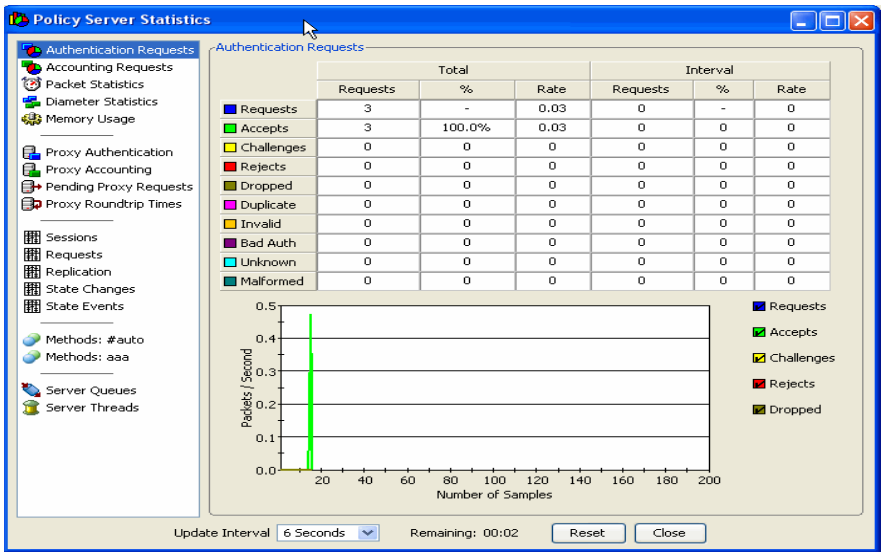
- Authentication Requests
- Accounting Requests
- Packet Statistics
- Diameter Statistics
- Memory Usage

The following sections explain in detail about these screens.

Authentication Requests

As shown in Figure 17-3, authentication requests are categorized according to status or **disposition**.

Figure 17-3 Server Statistics-Authentication Requests



This screen displays two groups of columns labeled **Total** and **Interval**. They display numerical values as follows:

The Total columns group displays the total count for the row since the last server reset.

The Interval columns group displays changes in counts since the last interval update. The update interval was set as shown in Figure 17-3.

The Total values are described in Table 17-2.

Table 17-2 Total Values

Column	Description
Requests	Current value of the counter.
%	Ratio of count to total number of requests.
Rate	The rate in the total column group represents the average number of requests per second since the last server reset.

The Interval values are described in Table 17-3.

Table 17-3 Interval Values

Column	Description
Requests	Current value of the counter.
%	Ratio of count to total number of requests.
Rate	The rate in the interval column group represents the average number of requests per second since the last interval update.

Authentication Statistics Counters are described in Table 17-4.

Table 17-4 Authentication Statistics Counters

Counter	Description of the Packet
Requests	The total number of valid RADIUS Access-Request packets received (Packet type 1).
Accepts	The number of Accept-Accept packets (Packet Type 2) sent to the RADIUS clients.
Challenges	The number of Accept-Challenge packets (Packet Type 11) sent to the RADIUS clients.
Rejects	The number of Accept Reject packets (Packet Type 3) sent to the RADIUS clients.
Dropped	The number of Access-Requests that were dropped (no response was sent).

Table 17-4 Authentication Statistics Counters

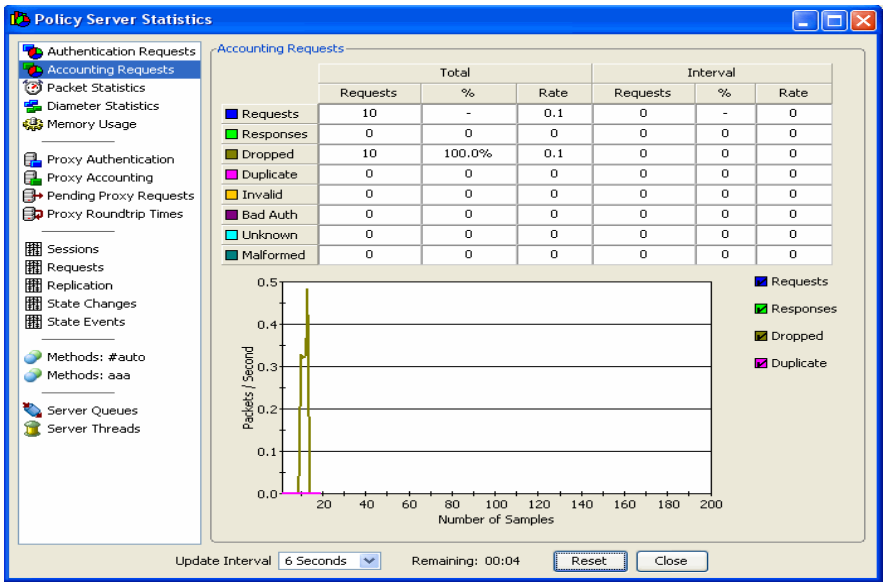
Counter	Description of the Packet
Duplicate	The number of Access-Request packets that matched another request which was already in the request queue (no response was sent for the duplicate request).
Invalid	The number packets received from unknown clients.
Bad Auth	The number of packets received which contained an invalid signature (authenticator).
Unknown	The number of packets received which did not match a known RADIUS RFC packet type.
Malformed	The number of packets received which contained data that could not be decoded.

The screen also displays a **performance monitor**. This is a graph that displays the number of packet samples (horizontal scale) against packets per update interval (vertical scale). The graph can show up to five types of authentication request based on disposition. Select or clear the appropriate checkbox to control this display.

Accounting Requests

Figure 17-4 shows the screen for monitoring accounting requests. It displays a columnar information and a performance monitor (graph) organized in the same manner as the Authentication Request screen.

Figure 17-4 Server Statistics-Accounting Requests



The columns are used in the same way as with authentication requests (Table 17-2). The requests are sorted according to accounting disposition, as described in Table 17-5.

Table 17-5 Accounting Disposition

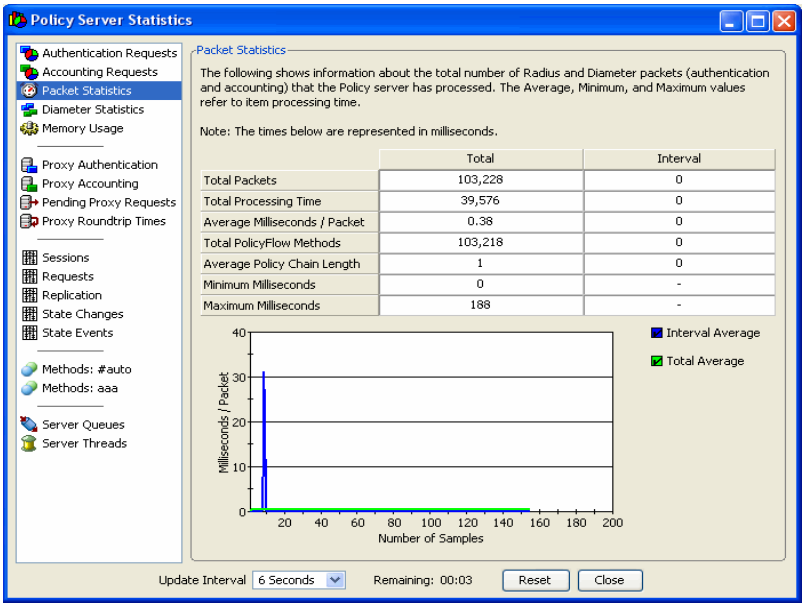
Disposition	Description of the Packet
Requests	The total number of valid Accounting-Request packets received (Packet type 4).
Responses	The number of Accounting-Acknowledgment packets sent (Packet type 5).
Dropped	The number of Accounting-Request packets that were dropped (no response was sent).
Duplicate	The number of Accounting-Request packets that matched another request which was already in the request queue (no acknowledgement was sent for the duplicate request).
Invalid	The number packets received from unknown clients.
Bad Auth	Associated with an authenticator that could not be verified.
Unknown	The number of packets received which did not match a known RADIUS RFC packet type.
Malformed	The number of packets received which contained data that could not be decoded.

The screen also displays a **performance monitor**. This is a graph that displays the number of packet samples (horizontal scale) against packets per update interval (vertical scale). The graph can show up to four types of accounting request based on disposition. Select or clear the appropriate checkbox to control this display.

Packet Statistics

Figure 17-5 shows the screen for monitoring packet statistics. It displays columnar information and a performance monitor (graph) in an organized manner.

Figure 17-5 Server Statistics-Packet Statistics



There are two columns:

- The **Total** column displays count and time statistics for all requests and responses processed since the server was last restarted or since the statistics panel was last reset.
- The **Interval** column displays the same information for packets received during the last update interval only. The update interval was set as shown in Figure 17-5.

The tabulated data is described in Table 17-6.

Table 17-6 Radius Items-Tabulated Items

RADIUS Item	Description
Total Packets	The total number of authentication and accounting packets combined.
Total Processing Time	The total amount of time spent processing authentication and accounting packets combined, in milliseconds.

Table 17-6 Radius Items-Tabulated Items

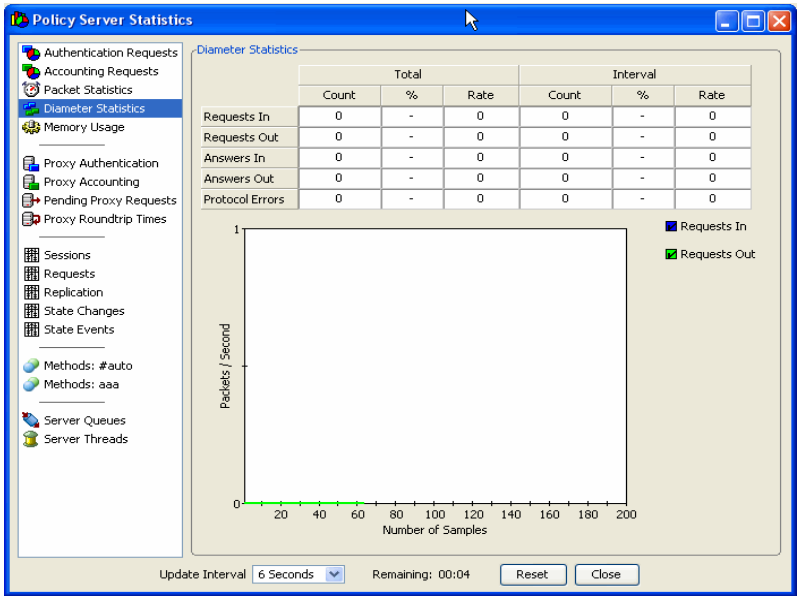
RADIUS Item	Description
Average Milliseconds / Packet	Average (Mean) rate of amount of taken to process a packet.
Minimum Milliseconds	Least amount of time spent processing a single packet.
Maximum Milliseconds	Greatest amount of time spent processing a single packet.

The **performance monitor** can be used to display current information regarding the average rate of processing a packet within the defined interval or based on total packets processed. Select one or both checkboxes to display the graphical data.

Diameter Statistics

Figure 17-6 shows the screen for monitoring diameter statistics. It displays a columnar information and a performance monitor (graph).

Figure 17-6 Server Statistics-Diameter Statistics



There are two columns **Total** and **Interval** which keeps the count of total number of requests flowing from and to the diameter server.

The tabulated data is described in the Table 17-7.

Table 17-7 Diameter Items-Tabulated Items

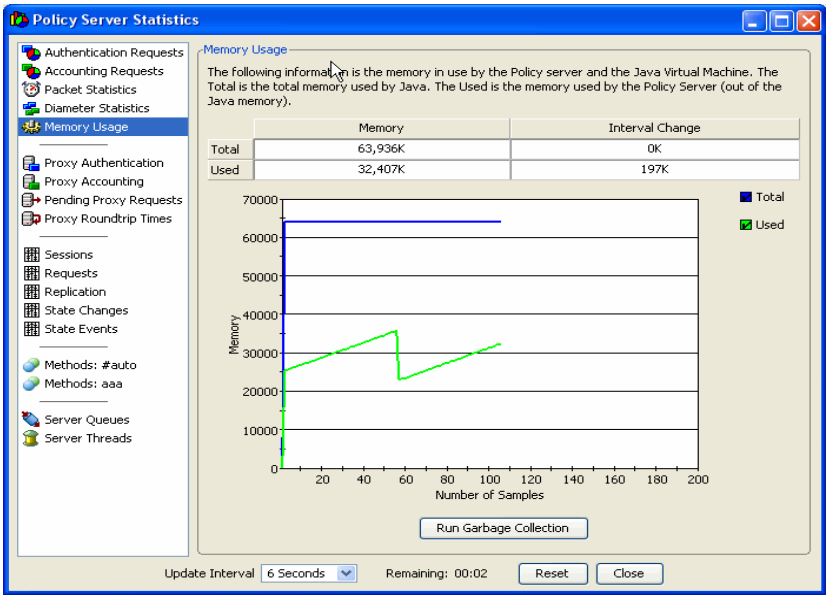
Diameter Item	Description
Requests In	Number of request received by the diameter server.
Requests Out	Number of requests sent by the diameter server to another diameter server.
Answers In	Number of requests answered by other diameter servers in response to the requests sent by a diameter sever.
Answers Out	Number of requests answered by the diameter server in response to the requests received by it.
Protocol Errors	Errors occurring during sending a or answering a request (Due to errors in any of the attributes).

Memory Usage

This screen provides information regarding the amount of memory used by the 8950 AAA server and the Java Virtual Machine (JVM). Memory is expressed in kilobytes.

Data is displayed within a table and a graph that memory usage over time. Figure 17-7 shows the screen.

Figure 17-7 Server Statistics-Memory Usage



In the table, the Memory column shows total memory used by the Java Virtual Machine (JVM) and the amount of memory currently in use by the 8950 AAA within the JVM.

The values in the Interval Change column are updated with each interval update. It shows the amount of change, if any, that occurred during the last update interval.

The screen also displays a graph showing the amount of memory usage (vertical scale) over time, in update intervals (horizontal scale). The monitor can show total JVM memory size and the amount of memory currently used by 8950 AAA. Select or clear the appropriate checkbox to control this display.

> **Important!** Used memory refers to the amount of memory in use by 8950 AAA within the JVM only.

Screens that Monitor RADIUS Requests Sent to Other Servers

This sections describes the following four screens:

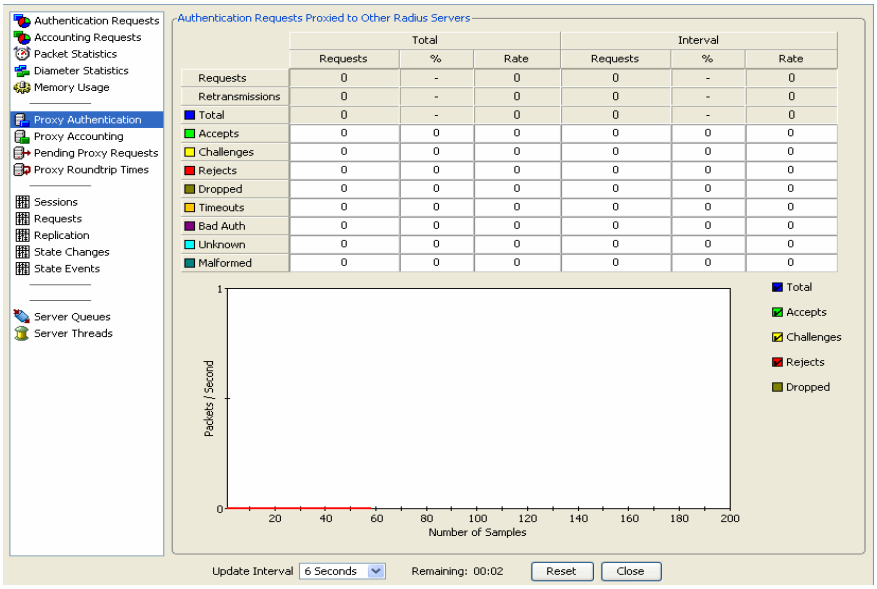
- Proxy Authentication
- Proxy Accounting
- Pending Proxy Requests
- Proxy Roundtrip Times

The following sections explain in detail about these screens.

Proxy Authentication

The Proxy Authentication screen displays information regarding authentication requests that have been sent to other servers for processing. Proxy authentication requests are categorized according to status or disposition.

Figure 17-8 Server Statistics-Proxy Authentication



As with other screens, this screen displays two groups of columns labeled **Total** and **Interval**. They display numerical values as follows:

- The Total columns display statistics about all packet types received by other servers.
- The Interval columns display disposition statistics for requests received during the last update interval.

The columns are used in the same way as with authentication requests.

Categories of proxy authentication requests are described in Table 17-8.

Table 17-8 Categories of Proxy Authentication requests

Category	Description of the Packet
Requests	Valid RADIUS Access-Request packets (Packet type 1).
Retransmissions	Additional Access-Request packets sent as a result of a time out.
Accepts	Access-Request packets that resulted in an Access-Accept (Packet Type 2) being returned to the RADIUS client.

Table 17-8 Categories of Proxy Authentication requests

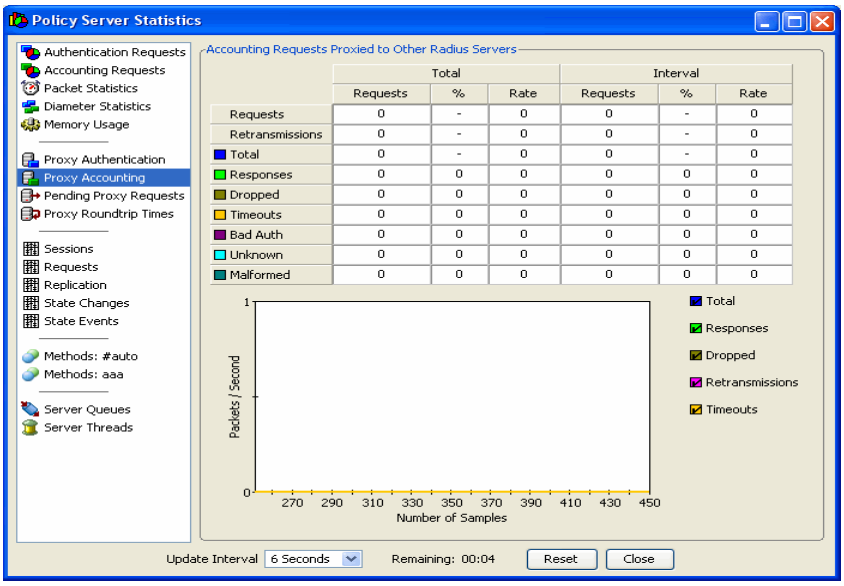
Category	Description of the Packet
Challenges	Access-Request packets that resulted in an Access-Challenge (Packet Type 11) being returned to the RADIUS client.
Rejects	Access-Request packets that resulted in an Access-Reject (Packet Type 3) being returned to the RADIUS client.
Dropped	Access-Request packets that resulted in the original request being dropped (no response was sent to the client).
Timeouts	Access-Request packets for which there was no answer received from the remote RADIUS server.
Bad Auth	Access-Request packets for which the response from the remote RADIUS server contained an invalid signature (authenticator).
Unknown	Access-Request packets for which the response from the remote RADIUS server did not match a known RADIUS RFC packet type.
Malformed	Access-Request packets for which the response from the remote RADIUS server contained data that could not be decoded.

The screen also contains a **performance monitor** which displays the number of packet samples (horizontal scale) over time, per update interval (vertical scale).

Proxy Accounting

The Proxy Accounting screen displays information regarding accounting requests that are sent to servers other than the 8950 AAA server.

Figure 17-9 Server Statistics-Proxy Accounting



As with other screens, this screen displays two groups of columns labeled **Total** and **Interval**. They display numerical values as follows:

- The Total columns display statistics about all packet types received by other servers.
- The Interval columns display disposition statistics for requests received during the last update interval.

The columns are used in the same way as with authentication requests.

Categories of proxy accounting requests are described in Table 17-9.

Table 17-9 Categories of Proxy Accounting requests

Category	Description of the Packet
Requests	Valid RADIUS Access-Request packets (Packet type 4).
Retransmissions	Additional Access-Request packets sent as a result of a time out.
Responses	Acknowledged valid RADIUS Access-Request packets (Packet type 5).
Dropped	Access-Request packets that resulted in the original request being dropped (no response was sent to the client).
Timeouts	Access-Request packets for which there was no answer received from the remote RADIUS server.

Table 17-9 Categories of Proxy Accounting requests

Category	Description of the Packet
Bad Auth	Access-Request packets for which the response from the remote RADIUS server contained an invalid signature (authenticator).
Unknown	Access-Request packets for which the response from the remote RADIUS server did not match a known RADIUS RFC packet type.
Malformed	Access-Request packets for which the response from the remote RADIUS server contained data that could not be decoded.

The screen also displays a **performance monitor** which is a graph that displays the number of packet samples (horizontal scale) against packets per second (vertical scale). The graph can show up to five types of proxy accounting requests based on disposition. Select or clear the appropriate checkbox to control this display.

Pending Proxy Requests

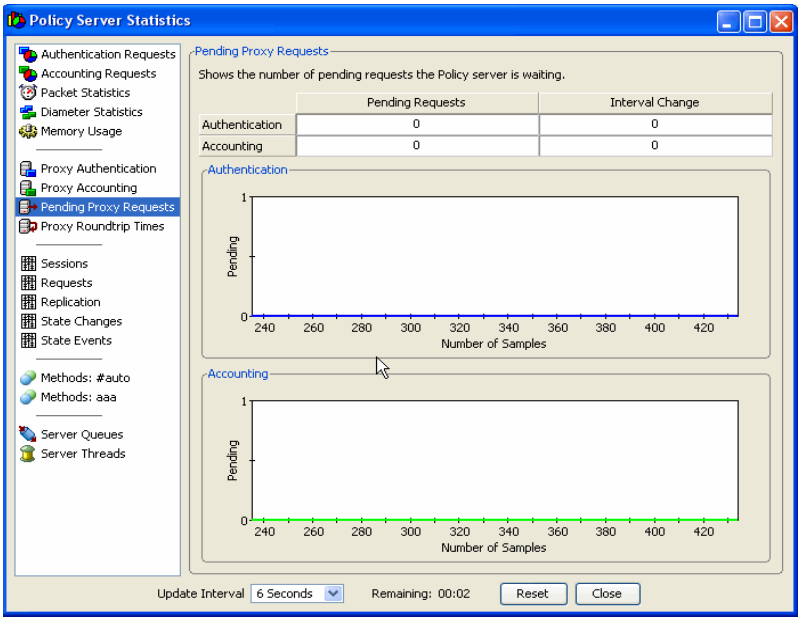
This screen is used to keep track of authentication and accounting requests that have been sent to other servers and for which the 8950 AAA server is waiting for status. It is shown in Figure 17-10.

Data is expressed both in tabular form and through performance monitors, one for proxy authentication requests and one for proxy accounting requests.

The screen contains two columns as follows:

- **Pending Requests**–Total number of pending proxy requests (waiting for a response).
- **Interval Change**–number of pending proxy requests sent since the last interval update.

Figure 17-10 Server Statistics-Pending Proxy Requests

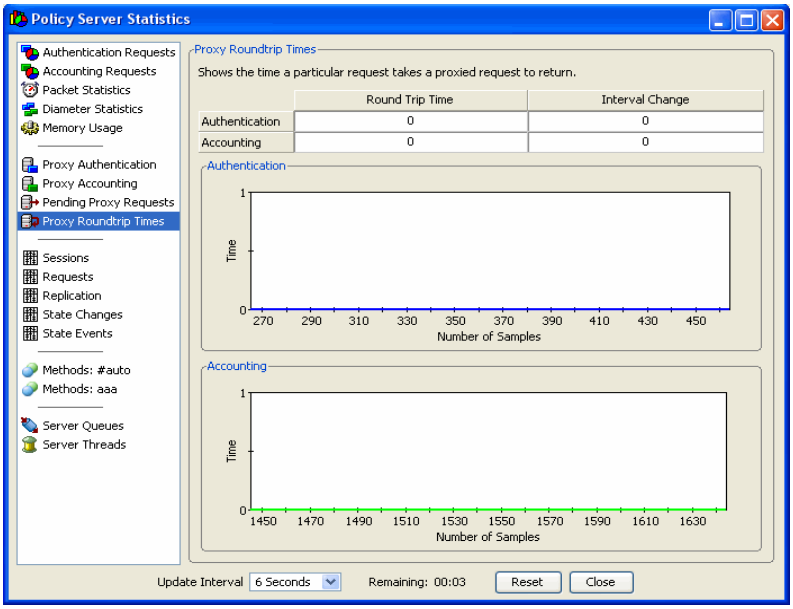


The screen also displays two **performance monitors** or graphs that display the number of packet samples (horizontal scale) against wait time in seconds (vertical scale).

Proxy Roundtrip Times

This screen is used to track the time required for proxy authentication and proxy accounting requests to return to the 8950 AAA server. The time measurement starts when the request is sent and ends when the response is received is shown in Figure 17-11.

Figure 17-11 Server Statistics-Proxy Roundtrip Times



Data is expressed both in tabular form and through performance monitors, one for proxy authentication requests and one for proxy accounting requests.

The screen contains two columns as follows:

- **Round Trip Time**–Total time spent waiting for responses to proxy authentication and proxy accounting requests since system initialization.
- **Interval Change**–Total time spent waiting for responses to proxy authentication and proxy accounting requests since the last interval update.

Each column contains an entry for proxy authentication requests and an entry for proxy accounting requests.

The screen also displays two **performance monitors** or graphs that display the number of packet samples (horizontal scale) against round trip time in seconds (vertical scale).

Screens that Monitor State Server Activity

This sections describes the following four screens:

- Sessions
- Requests
- Replication
- State Changes
- State Events

The following sections explain in detail about these screens.

Sessions

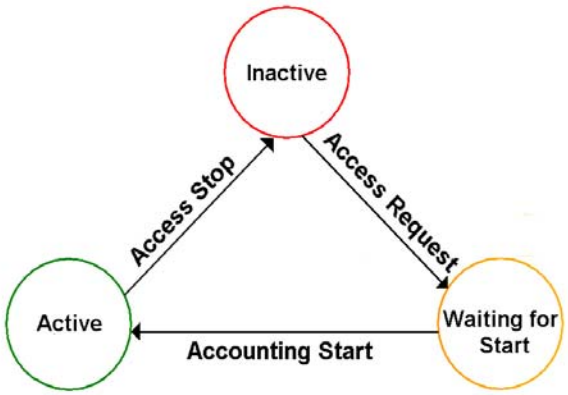
The State Server Sessions screen is used to monitor the 8950 AAA Universal State Server (USS). It contains three tabs and one performance monitor, as shown in Figure 17-13.

To the USS, a network session is an occupied port on a specific client. A session is defined by a series of RADIUS requests that pertain to the particular port and client. The performance monitor displays graphical data for monitoring up to three types of sessions:

- **Active Sessions**–Sessions that are currently running.
- **Inactive Sessions**–Sessions that have terminated.
- **Waiting for Start**–Sessions that have been authenticated but for which no accounting Start record has been received.

Below is a graphical depiction of the session types.

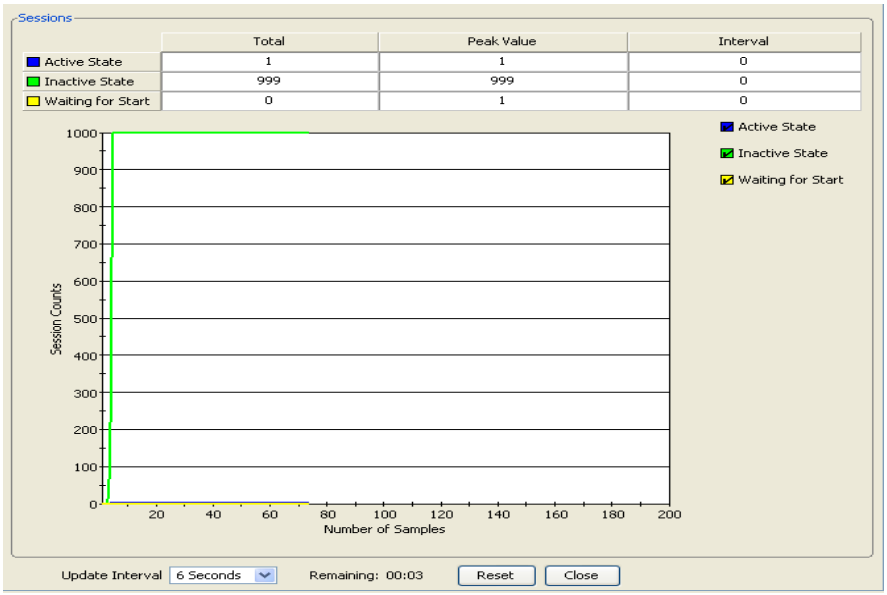
Figure 17-12 Session State-Life cycle of a Session



The State Server screen tabs are described below.

The Sessions window is shown in Figure 17-13.

Figure 17-13 Server Statistics-Sessions



It contains three columns used for displaying tabular data with respect to the three types of sessions. They are described in Table 17-10.

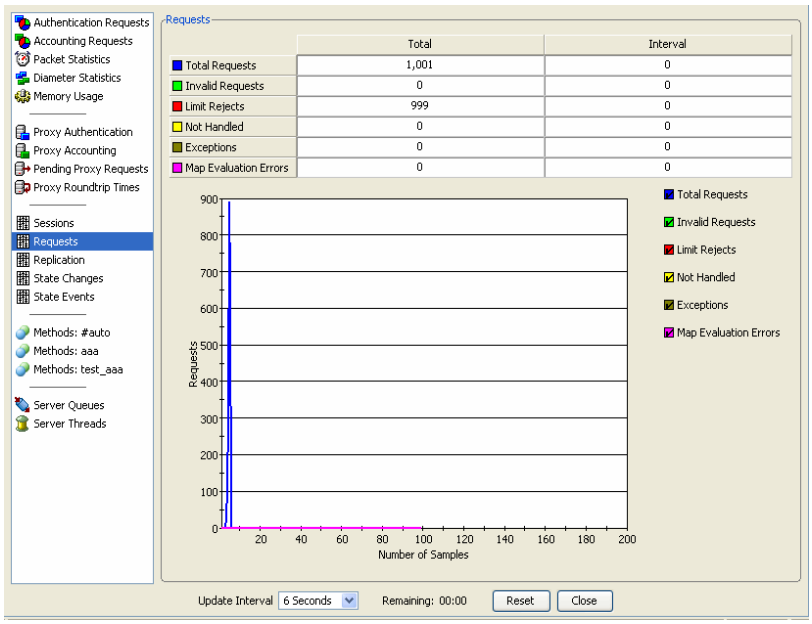
Table 17-10 State Server-Sessions Tab properties

Column Name	Description
Total	Total number of sessions of each type since the State Server was initialized.
Peak Value	High water mark indicating the greatest number of sessions since the State Server was initialized.
Interval	Total number of sessions of each type since the last interval update.

Requests

The State Server Requests window is shown in the Figure 17-14.

Figure 17-14 Server Statistics-Requests



It provides tabular data regarding different requests to the State Server. Data is arranged in two columns labeled **Total** and **Interval**. They display numerical values as follows:

- The Total column displays a count of packets since server initialization.
- The Interval column displays a count of packets since the last interval update.

The types of requests are described in Table 17-11.

Table 17-11 State Server-Request Tab properties

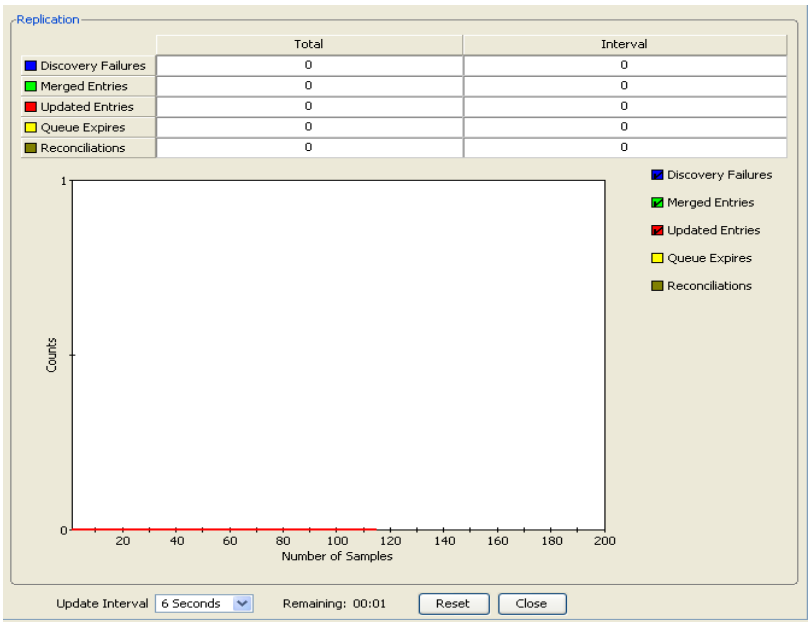
Request Types	Description
Total Requests	Amount of state server requests.
Invalid Requests	Amount of state server requests that could not be processed due to error in request.
Limit Rejects	Amount of state server requests that surpassed the resource use limit.
Not Handled	Count of Accounting-Requests that are too old because newer information has been received.
Exceptions	Amount of state server requests that could not be processed due to general exception faults.
Map Evaluation Errors	Count of interval PolicyFlow errors.

Replication

The Replication screen displays the status of replicated sessions.

Figure 17-15 displays the Replication screen.

Figure 17-15 Server Statistics: Replication



Data is displayed in columns and through a performance monitor (graph).

There are two columns:

- The Total column displays the count of replicated sessions since server initialization.
- The Interval column displays a count of replicated sessions since the last interval update.

The categories of replication are described in the Table 17-12.

Table 17-12 State Server-Replication Tab properties

Request Types	Description
Discovery Failures	Status of secondary server discovery.
Merged Entries	Number of entries merged with the secondary server.
Updated Entries	Number of entries updated before reaching the secondary server.
Queue Expires	Expiration of entries.
Reconciliations	Collection of entries which are not updated or merged on the primary server.

The **performance monitor** displays the number of samples (horizontal scale) per count (vertical scale).

State Changes

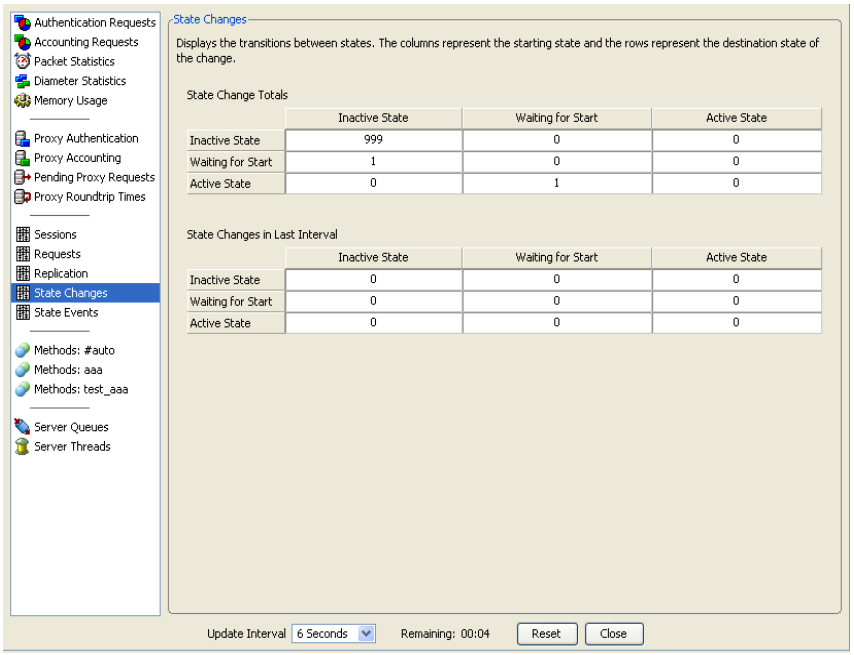
Transitions between stages are monitored through the State Change screen as shown in Figure 17-16.

There are two panes **State Change Total** which displays the total state changes and **State Changes in Last Interval** which displays the state change which occurred in the last interval.

Every session consists of three basic stages:

- Active State
- Inactive State, or
- Waiting for Start

Figure 17-16 Server Statistics-State Changes



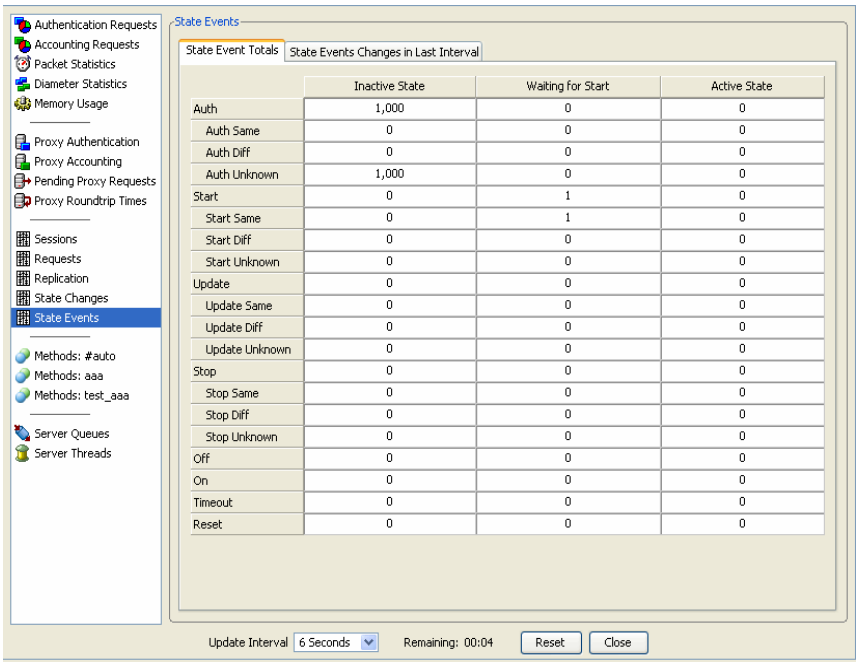
State Events

Every session reports on the server events via the 8950 AAA Server Statistics. Below is an example of how the events are presented. There are two tabs namely **State Change Total** and **State Changes in Last Interval** (See Figure 17-17)

The events are in one of the following states:

- Active State
- Inactive State
- Waiting for Start

Figure 17-17 Server Statistics-State Events



Screens that Monitor State Server Activity

This sections describes the following two screens:

- Methods: #auto
- Methods: aaa

Each screen provides the ability to monitor the methods that are called during PolicyFlow processing. Methods are monitored in four ways as shown in Table 17-13.

Table 17-13 Types of Methods

Measurement	Description
Processing Rate	Average rate for executing this method in calls per millisecond.
Processing Period	Average time it takes for executing this method in milliseconds per call.
Invocation Count	Number of times this method was called.
Processing Time	Total time spent executing this method.

Using these four criteria, the methods are analyzed for each possible method **disposition** or state. The dispositions are described in Table 17-14.

Table 17-14 Method Dispositions

Disposition	Description
Total	Total time spent executing the method OR total number of times that the method was called.
Success	Method completed its task and execution passed to the method, if any, named in the *Method-Next* control property.
Fail	Method failed to complete its task and execution passed to the method, if any, named in the *Method-On-Fail* control property.
Error	Method encountered an error and could not correctly perform its task. Execution passed to the method, if any, named in the *Method-On-Fail* control property.
Accept	Method forced an immediate *Accept* in the 8950 AAA packet engine.
Reject	Method forced an immediate *Reject* in the 8950 AAA packet engine.
Discard	Method forced an immediate *Discard* in the 8950 AAA packet engine.
Suspend	Method ended in a suspended state waiting for the result of another process. Currently only the Radius plug-in can generate this disposition.
Jump	Method directed processing to another method, using *Branch* or *Goto*.
Challenge	Method generated an Access-Challenge packet (*Packet Type 11*) and ended.
Timeout	Time-out period that was set in the method control *Timeout* property was exceeded.

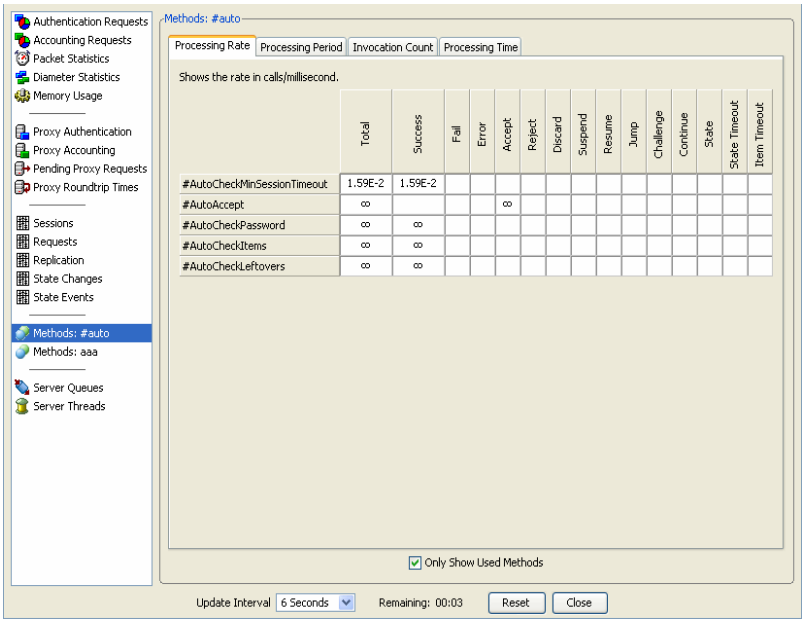
Each screen contains four tabs, one for each of the measuring criteria used for comparing method utilization. Each tab contains a table that lists method data based on method disposition. Figure 17-18 shows the Methods: #auto screen with the Processing Rate tab selected.

Important! One method invocation can produce entries in more than one column. For example, a method that results in a Time-out also counts as an Error, as well as being counted in the Total column.

The following sections display each of the four tabs on the Methods: #auto screen and the Methods: aaa screen.

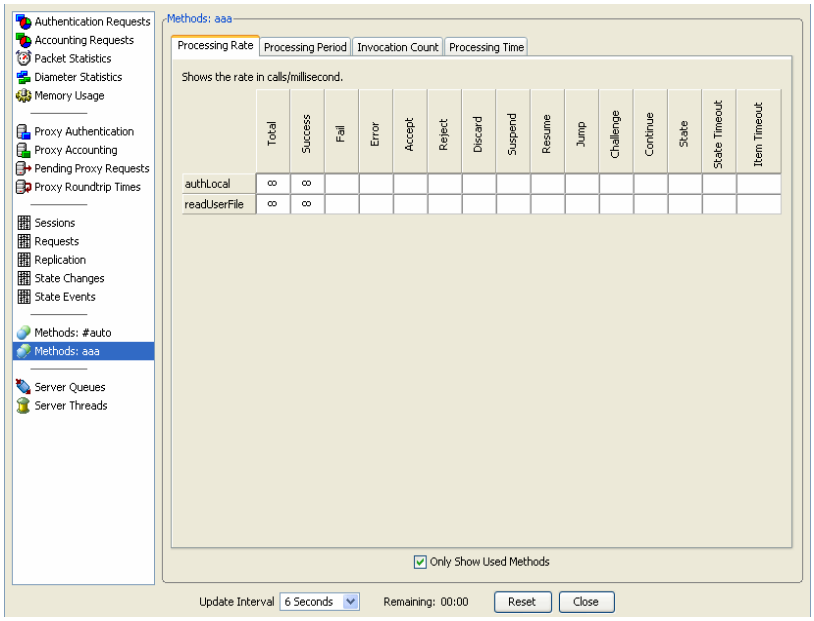
Methods: #auto

Figure 17-18 Server Statistics–Methods: #auto



Methods: aaa

Figure 17-19 Server Statistics–Methods: aaa



Screens that Monitor Internal Server Processing

This sections describes the following two screens:

- Server Queues

- Server Threads

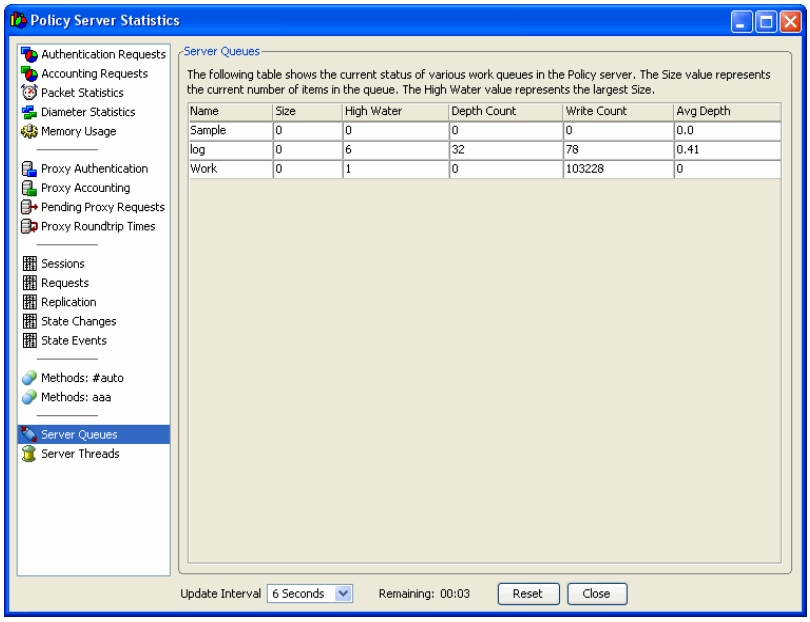
Server Queues

Queues are used for collecting data that needs to be processed. The Server Queues screen (Figure 17-20) is used to monitor queue status. This screen contains information as described in Table 17-15.

Table 17-15 Server Queues

Attribute	Description
Name	Identifies the specific server queue.
Size	Current number of enqueued items.
High Water	Highest number of enqueued items up to now.
Depth Count	The count to which the queue is utilized.
Write Count	The number of times items are written into the queue.
Avg Depth	Average Depth (Depth Count/Write Count).

Figure 17-20 Server Statistics-Server Queues



Server Threads

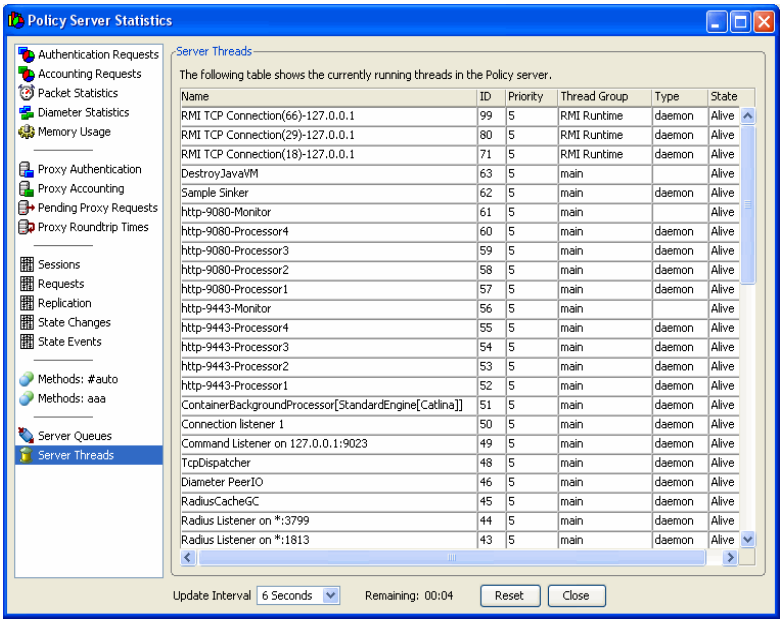
A thread is a code segment that can be executed simultaneously with other threads. At any given time, the 8950 AAA server executes multiple threads. The Server Threads screen (Figure 17-21) displays information about threads that are currently running.

Table 17-16 describes the information that is displayed about each running thread.

Table 17-16 Server Treads

Attribute	Description
Name	Identifies the thread.
ID	Thread identification number.
Priority	Number used for ranking the thread. A low value indicates a high rank.
Thread Group	Category based on how the thread is used.
Type	Category based on where the thread originated.
State	State of the thread.

Figure 17-21 Server Statistics-Server Threads



Sessions/ Counters/ Indices Panel

Sessions/Counters/Indices Panel

The Ports/Counters panel monitors three properties of the 8950 AAA Universal State Server (USS): **sessions**, **counters,** and **indices**.

Counters are created and maintained by the USS. Each counter tracks the occurrences of a specific resource and contains the number of active sessions using that resource. For example, if the counter for the resource *User-Name=axrippa* is 2, that means there are two active sessions on the network for which the *User-Name=axrippa*.

Counters may be used to enforce PolicyFlow resource limit policies on the 8950 AAA server.

To display the Sessions/Counters/Indices panel, use the SMT Navigation Pane to select **Sessions/Counters/Indices** under Monitoring Tools, as shown in Figure 17-22.

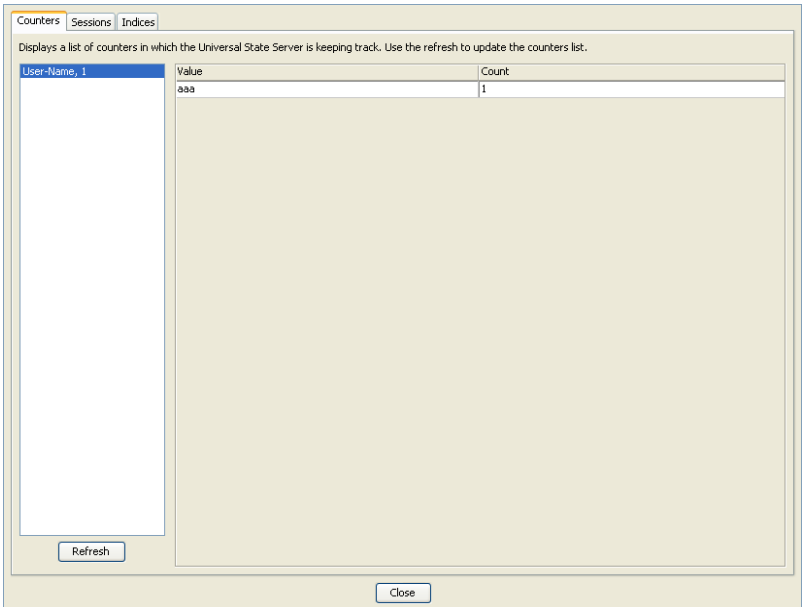
Figure 17-22 Navigation Pane-Sessions/Counters/Indices

The Sessions/Counters/Indices panel appears as shown in Figure 17-23.

The Counters tab displays a list on the left side. Each list entry contains a **value** and a **count** of sessions associated with that counter.

Click **Refresh** to update the counters list.

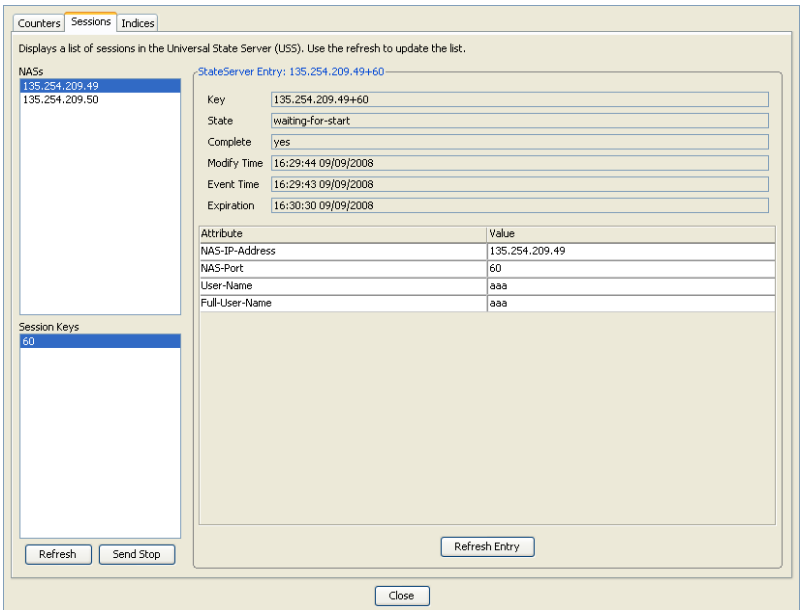
Figure 17-23 Sessions/Counters/Indices-Counters Tab



The Sessions tab is shown in the Figure 17-17.

The list of sessions (IP- address under **NASs** and session key under **Session Keys**) is displayed on the left side and corresponding state server entry is displayed on the right side of the panel.

Table 17-17 Sessions/Counters/Indices-Sessions tab



Use **Refresh** to update the NAS and Session key list.

Click **Send Stop** to stop or inactivate the selected NAS and Session key.

Use the **Refresh Entry** to update the state server entries.

The state server entry attributes are described in the Table 17-18.

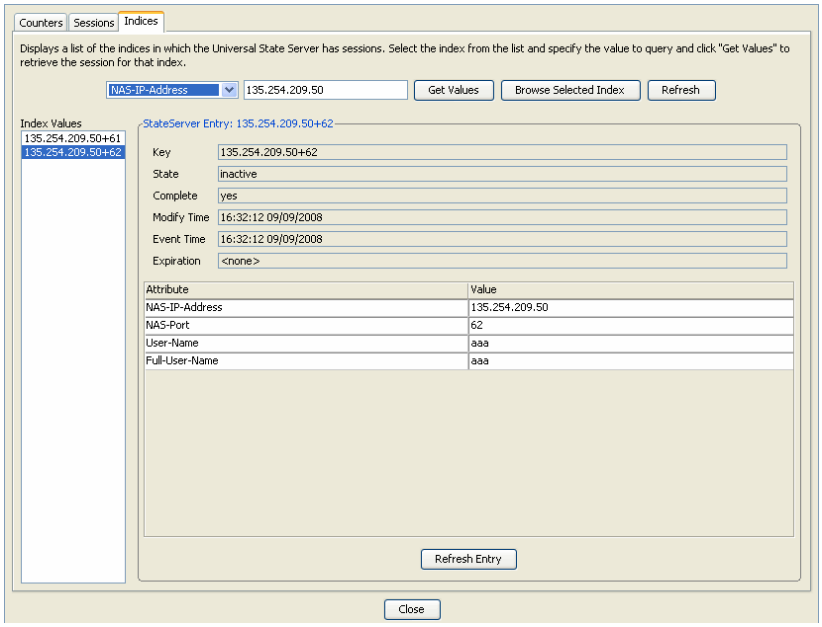
Table 17-18 State Server Entry

Attribute	Description
Key	The session key.
State	The current state of the session.
Complete	The progress of the session.
Modify Time	Modification time.
Event Time	Start of the event.
Expiration	The time of expiration.

The Indices tab is shown in Figure 17-24. It displays a list of indices with which the USS has active sessions. Select the index from the list and click **Get Values** to display the corresponding State Server Entry.

The **Attribute** and **Value** columns below display the IP-address, port-ID, user-name, and the full user name.

Figure 17-24 Sessions/Counters/Indices-Indices Tab



The State Server Entry attributes are same as in Sessions tab.

Click **Browse Selected Index** to select other IP addresses.

USS Address Statistics Panel

Sessions/Counters/Indices Panel

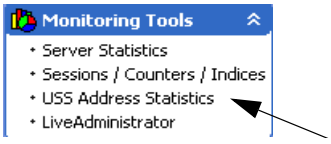
The USS Address Statistics panel monitors the address statistics of 8950 AAA Universal State Server (USS).

The USS addresses are created and maintained by the USS. The Address Pool is configured using the USS Address Manager panel.

USS Address Statistics panel displays the statistics of the addresses selected from the Pool.

To display the USS Address Statistics panel, use the SMT Navigation Pane to select **USS Address Statistics** under Monitoring Tools, as shown in Figure 17-25.

Figure 17-25 Navigation Pane-USS Address Statistics



The USS Address Statistics panel is displayed, as shown in Figure 17-26.

Figure 17-26 USS Address Statistics Panel

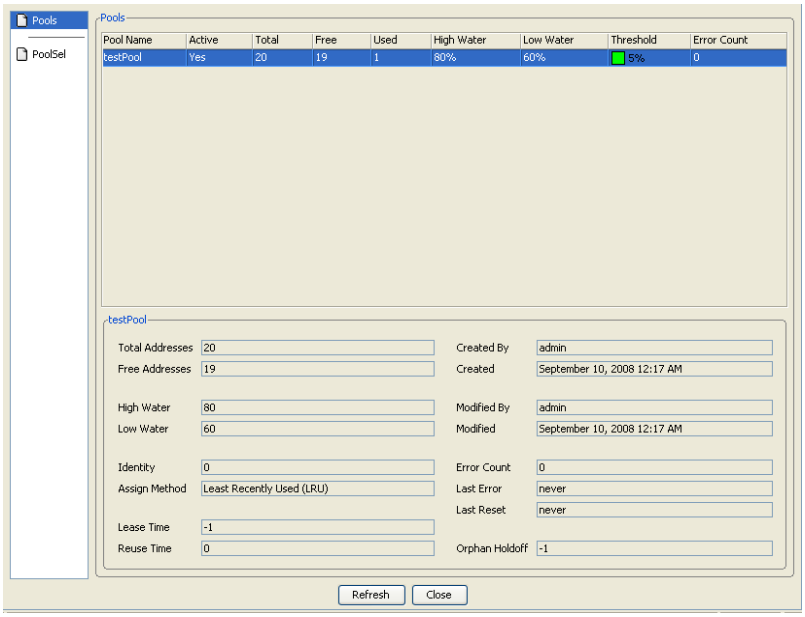


Table 17-19 Pools

Attribute	Description
Pool Name	Name of the Pool.
Active	State of the pool (active or not).
Total	Total addresses in the pool.
Free	Number of free addresses in the pool.
Used	Number of used addresses in the pool.
High Water	Specifies the maximum percentage of available pool addresses.
Low Water	Specifies the minimum percentage of available pool addresses
Threshold	Specifies the current percentage of available pool addresses.
Error Count	Number of errors occurred.

A detail description of the pool selected is shown in the below portion.

END OF STEPS

18 Using LiveAdministrator

Overview

Purpose

This section provides information about the 8950 AAA LiveAdministrator and some of the terms that you will encounter when working with the 8950 AAA product.

The following topics are included in this chapter:

8950 AAA LiveAdministrator

Live Administrator

Use the LiveAdministrator panel to manage, diagnose and control an operational 8950 AAA server. LiveAdministrator provides a graphical user interface that enables the following:

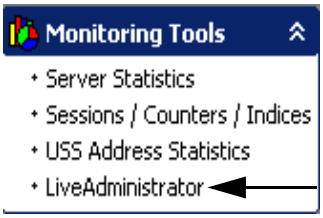
- Display of server settings
- Modification of server settings
- Display server statistics
- Display and modify some stored data
- Pause and resume server operations
- Control logging operations
- Capture server setting information in a text file

Accessing the LiveAdministrator Panel

Accessing Live Administrator

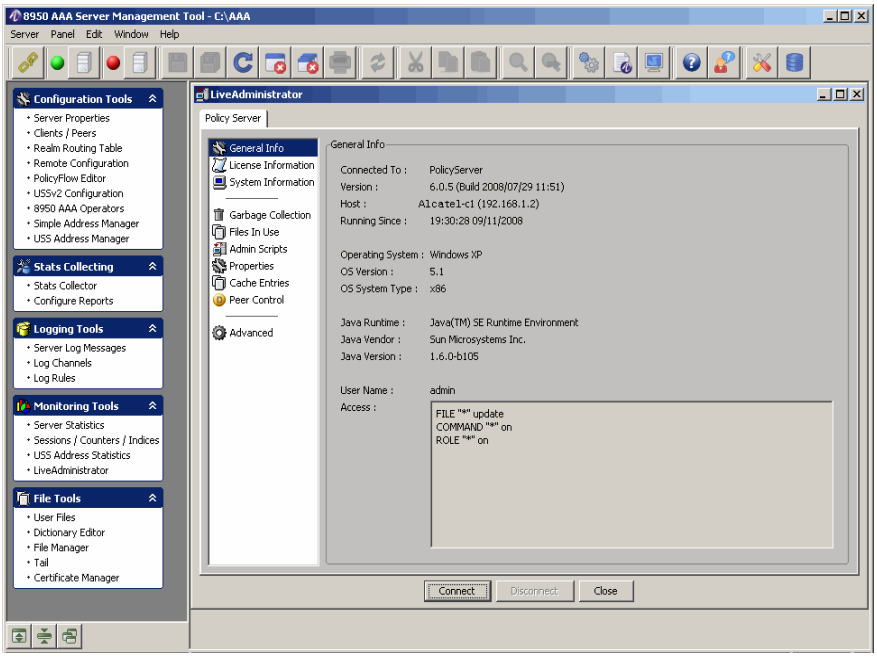
Using the SMT, select **LiveAdministrator** under **Monitoring Tools**, from within the Navigation Pane, as shown in Figure 18-1.

Figure 18-1 Navigation Pane-Live Administrator



The LiveAdministrator panel appears as shown in Figure 18-2.

Figure 18-2 8950 AAA LiveAdministrator Panel



This panel contains a list of administrative options (on the left-hand side) and a work area on the right-hand side. Select an option name to display the corresponding work area. The appropriate work area appears on the right side. There are three buttons in the bottom of the panel. Click the **Close** button to close the LiveAdministrator panel. Click the **Connect** button to connect to the Policy server, Configuration server, or to any other port. Click the **Disconnect** button to disconnect from the server(s) or port.

General Info

About General Information

Select **General Info** option to display the General Info work area. This is the default option that is displayed when you open Live Administrator panel and is displayed as shown in Figure 18-2.

This screen displays read-only information about the 8950 AAA server. Some of the fields are as described in Table 18-1.

Table 18-1 Live Administrator-General Info properties

Field Name	Description
Connected To	Displays the server that the 8950 AAA is currently connected to. Type, version, and legal information regarding the server.

Table 18-1 Live Administrator–General Info properties

Version	The Version number of 8950 AAA Server Management Tool (SMT).
Host	Name of host system.
Running Since	Time and date when the server was last started.
OS Version	The Operating System (OS) version.
OS System Type	The Operating System (OS) type.
Java Runtime	The Java Run time Environment information.
Java Vendor	The Java Vendor information.
Java Version	The Java version information.
User Name	The login name of the current admin user.
Access	Displays access permissions for the current admin user.

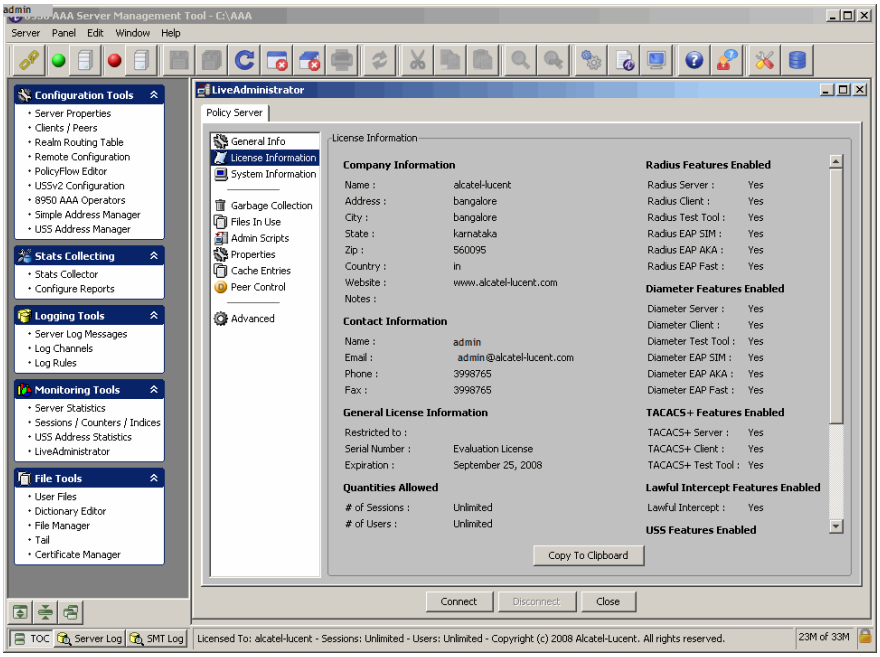
The first few fields display information that is set when the server is started and cannot be changed without restarting the server. The last information like the *User Name* and *Access*, is changed only by logging out of SMT and logging in again using a different administrative user account.

License Information

About License Information

Select **License Information** option to display the License information work area, as shown in Figure 18-3.

Figure 18-3 LiveAdministrator Panel-License Information



The work area appears on the right side displays license information about the 8950 AAA. Click the **Copy Properties to Clipboard** button to copy all entries to memory. Open a text file and paste the clipboard contents into the text file.

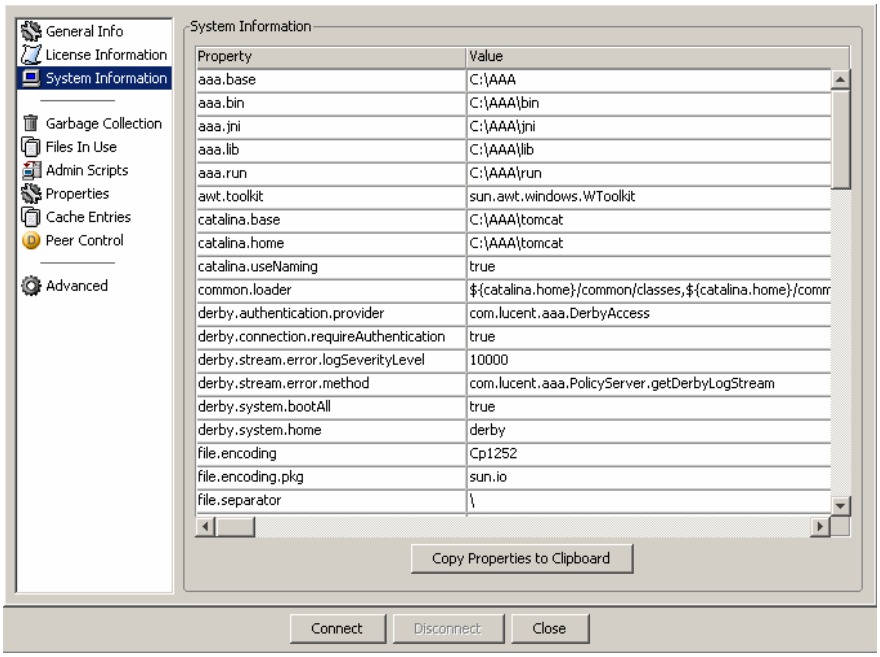
There are three buttons in the bottom of the panel. Click the **Close** button to close the LiveAdministrator panel. Click the **Connect** button to connect to the Policy server, Configuration server, or to any other port. Click the **Disconnect** button to disconnect from the server(s) or port.

System Information

About System Information

Select **System Information** option to display the System information in the corresponding work area, as shown in Figure 18-4. This work area displays a list of internal 8950 AAA property settings and their current values. These properties are set in the 8950 AAA scripts and the Java virtual machine. The work area allows the user to display and copy the properties from the list. The information displayed in this work area is read only.

Figure 18-4 LiveAdministrator Panel-System Information



To copy all entries to memory, click **Copy Properties to Clipboard**. Open a text file and paste the clipboard contents into the text file.

The work area appears on the right side displays system information about the 8950 AAA. Click the **Copy Properties to Clipboard** button to copy all entries to memory. Open a text file and paste the clipboard contents into the text file.

There are three buttons in the bottom of the panel. Click the **Close** button to remove the LiveAdministrator panel. Click the **Connect** button to connect to the Policy server, Configuration server, or to any other port. Click the **Disconnect** button to disconnect from the server(s) or port.

Garbage Collection

About Garbage Collection

Select **Garbage Collection** to display the corresponding work area as shown in Figure 18-5. The top portion of the work area displays information about memory usage for the Java Virtual Machine (JVM) within which 8950 AAA is running.

Figure 18-5 LiveAdministrator: Garbage Collection

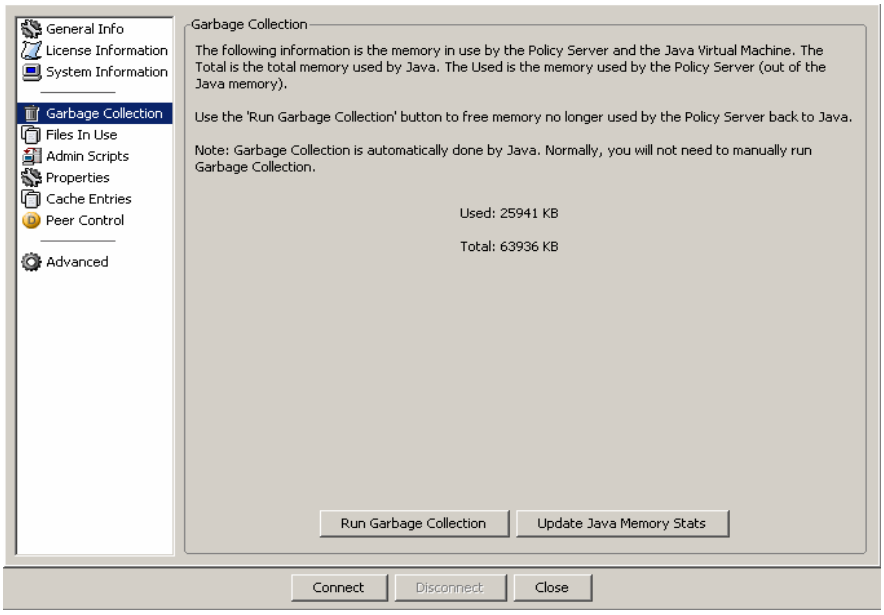


Table 18-2 Live Administrator–Garbage Collection properties

Field Name	Description
Used	Amount of JVM memory currently in use by 8950 AAA.
Total	Amount of memory available to the JVM.

This screen contains two buttons for managing memory. Click the **Run Garbage Collection** button to release memory that is no longer used by the server back to the JVM. Click the **Update Java Memory Stats** button to refresh the displayed information.

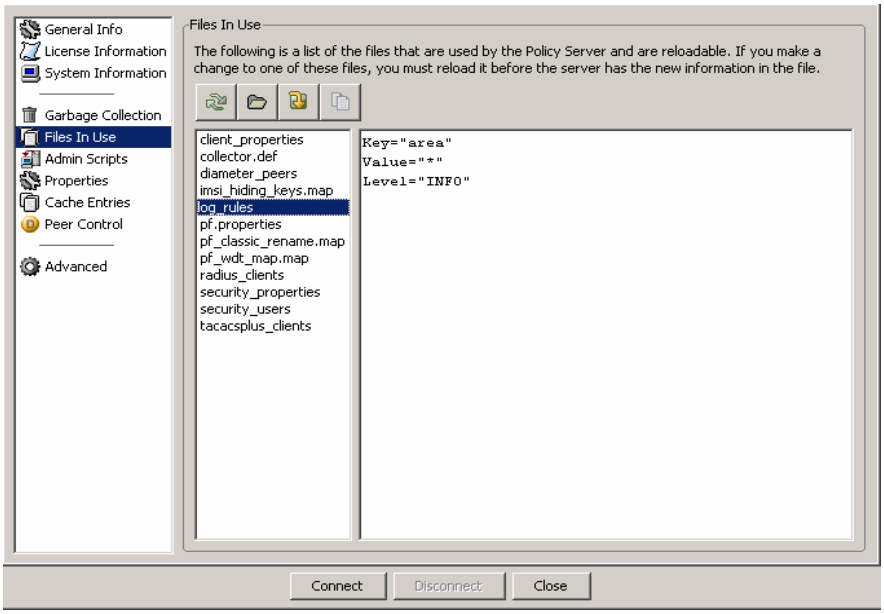
Important! Garbage collection is automatically managed by the Java Virtual Machine (JVM). You should normally not need to run garbage collection manually. Using the Universal State Server (USS) may be negatively affected by manual garbage collection.

Files in Use

About Files in use

Select **Files in Use** to display the corresponding work area as shown in Figure 18-6. This screen displays a list of files that have been read and are currently in use by the 8950 AAA server. The work area allows the user to display the contents of the selected file on the right side of the work area.

Figure 18-6 LiveAdministrator-Files in Use



The action buttons in the top of the panel allows you to perform required actions.

- 8950 AAA caches all file data in memory. Depending on the usage of the file, a file may be read and cached at server initialization or when the file is first referenced. If an open file has been modified it must be reloaded before 8950 AAA will see the changes. Click the **Reload** button, , to update the in-memory file contents of the selected file.
- To display the contents of a file, select the filename from the left side of the work area and click the **View File** button, , or double-click the file name.
- If the list of files used by 8950 AAA has changed, click **Update File List** button, , to refresh the list.
- To copy file contents to a text file, use the **View File** button to display the contents of the file, then, click **Copy to Clipboard** button, .You may then paste the copied text into another application.

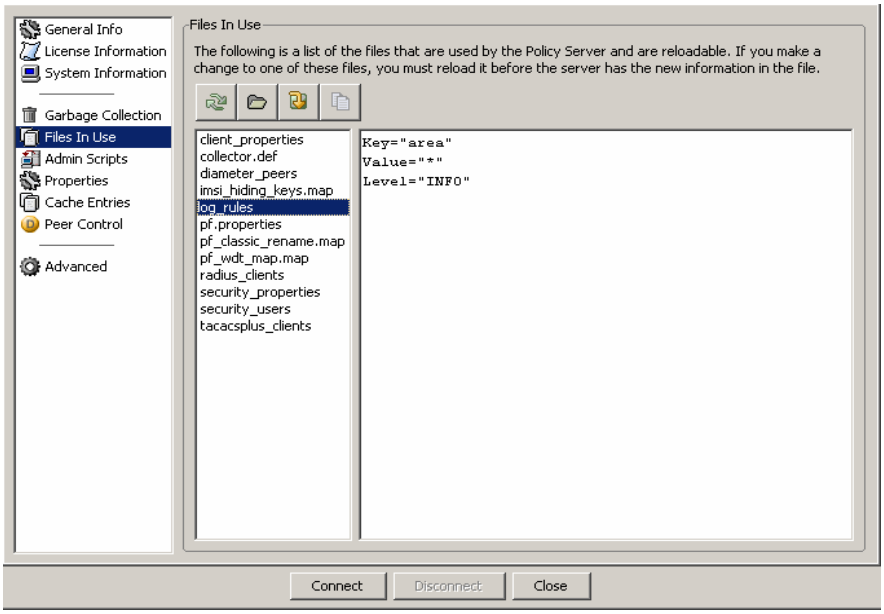
Important! While you can view files and copy their contents, you cannot edit the contents of a file from the LiveAdministrator.

Admin Scripts

About Admin Scripts

Select **Admin Scripts** to display the corresponding work area as shown in Figure 18-7. This work area displays a list of a wide range of administrative files used by the 8950 AAA server. These files may contain shell scripts, SQL commands, and PolicyFlow. The screen allows the user to display the contents of these files and to execute them as admin script files.

Figure 18-7 LiveAdministrator-Admin Scripts



Important! The LiveAdministrator can only execute Administrative Interface commands. It cannot execute shell scripts, PERL scripts, DOS batch files, and so on. However, the LiveAdministrator panel is unable to determine the contents of a file from its name. Therefore, when you tell the LiveAdministrator to execute a file it will attempt to execute each line in that file as though it were a legitimate administrative command. In this case, any properly formatted, syntactically correct administrative interface commend will be executed, while other commands and text will result in errors.

For this reason, it is best to only execute files that you are certain to contain legitimate administrative interface commands.

The action buttons in the top of the panel allows you to perform required actions.

- To display a script file's contents, select the filename from the left side and click the **View File** button,  .

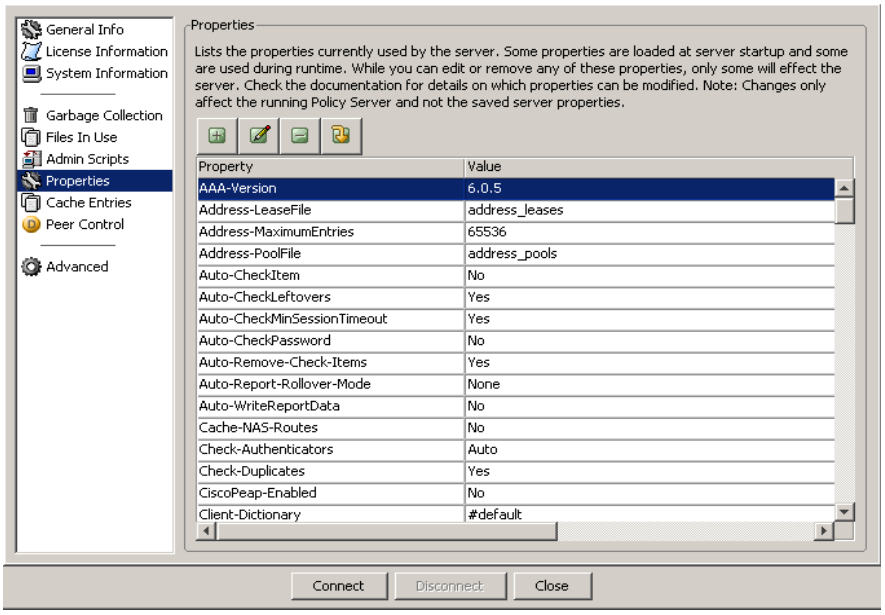
- To execute a script file, click **Run Script** button, ,to update the file contents. A message appears in the lower window of the work area displaying the results of the script execution.
- If the list of script files available to 8950 AAA has changed, click **Update File List** button, , to refresh the list.
- To copy file contents to a text file, use the **View File** button, , to display the contents of the file, then, click **Copy to Clipboard**, to copy the file contents to memory. Open a text file and paste the clipboard contents into the text file.

Properties

About Properties

Select **Properties** to display the corresponding work areas shown in Figure 18-8. This work area displays a list of server properties presently in effect and their current values. The screen allows the user to display, edit, add, and remove properties from the list. Server properties are normally defined and their values set in the SMT Server Properties panel. Server Properties may also be created, and their values set or changed through commands in the PolicyFlow. The Properties work area displays all currently defined Server Properties, regardless of how they were defined.

Figure 18-8 LiveAdministrator-Properties



Important! This property does persist beyond a server restart.

The action buttons in the top of the panel allows you to perform required actions.

- To define a new property and value, click the **Add** button,  . The Property dialog box appears in which there are fields for entering the new property and its value.

  Important! Some properties are only read at the time the 8950 AAA server is started. Changing these properties will have no effect on the running server. Changing or adding a property may have no effect if it is not understood by the server or referenced in the PolicyFlow.
- To modify an entry, click the **Edit** button,  . A dialog box appears in which modifications can be made.
- To remove the selected entry, click **Remove** button,  .

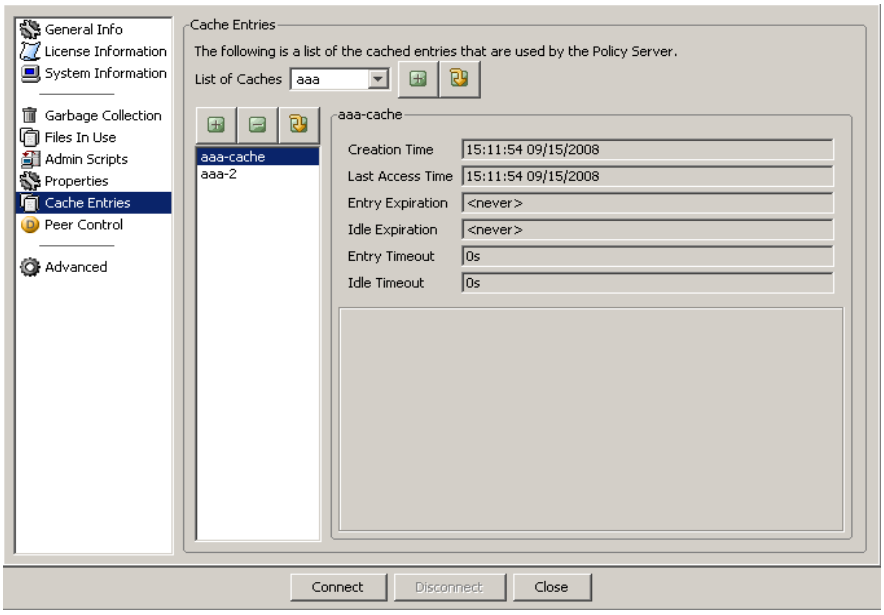
  Important! Decide carefully about removing an entry. There is no confirmation request and there is no undo operation. The only recovery is to restart the 8950 AAA server.
- To update the list of properties, click the **Refresh** button,  .

Cache Entries

About Cache Entries

Select **Cache Entries** to display the corresponding work area as shown in Figure 18-9. This work area displays a list of currently active 8950 AAA Cache Entries. These entries are normally set in the Policy Flow, though they can be set, modified and deleted through the administrative interface. The work area lets the user display, add and remove Cache Entries.

Figure 18-9 LiveAdministrator-Cache Entries



There are two sets of action buttons in this screen. The first set has two action buttons. These allow you to Add a Cache entry or refresh the list.

The second set of action buttons in the top of the panel allows you to perform required actions.

- To add a new entry to the cache, click the **Add** button, .
- To remove the selected entry, click the **Remove** button, .
- To update the list of cache entries, click the **Refresh** button, .

Important! Adding cache entries will only affect the current PolicyFlow if the PolicyFlow takes the values of the added entry into account in its internal logic.

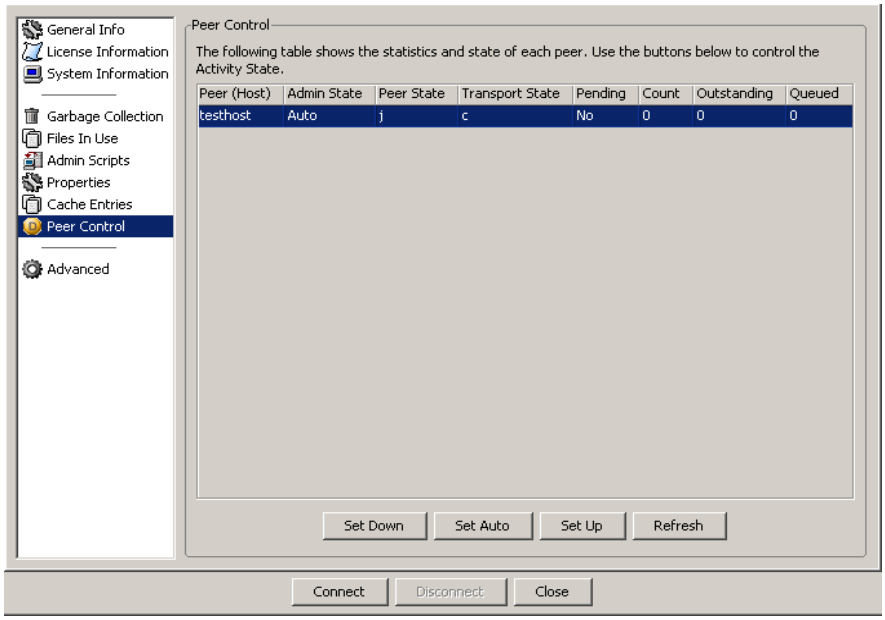
Peer Control

About Peer Control

Select **Peer Control** to display the corresponding work area as shown in Figure 18-10.

This work area displays the statistics and state of each peer. You can control the Activity State of these using the buttons in the bottom of the panel.

Figure 18-10 LiveAdministrator-Peer Control



There are four buttons in this screen that allows you to set the Activity State as required.

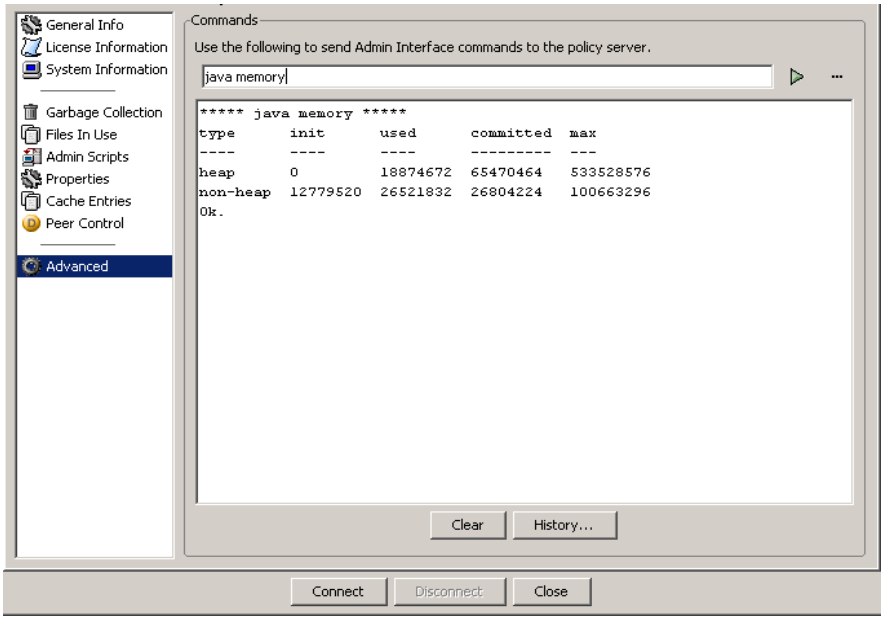
- To set the Activity State to Down, click the **Set Down** button.
- To set the Activity State to Auto, click the **Set Auto** button.
- To set the Activity State to Up, click the **Set Up** button.
- To refresh the screen, click the **Refresh** button.

Advanced

About Advanced

Select **Advanced** to display the Commands screen as shown in Figure 18-11.

Figure 18-11 LiveAdministrator-Advanced



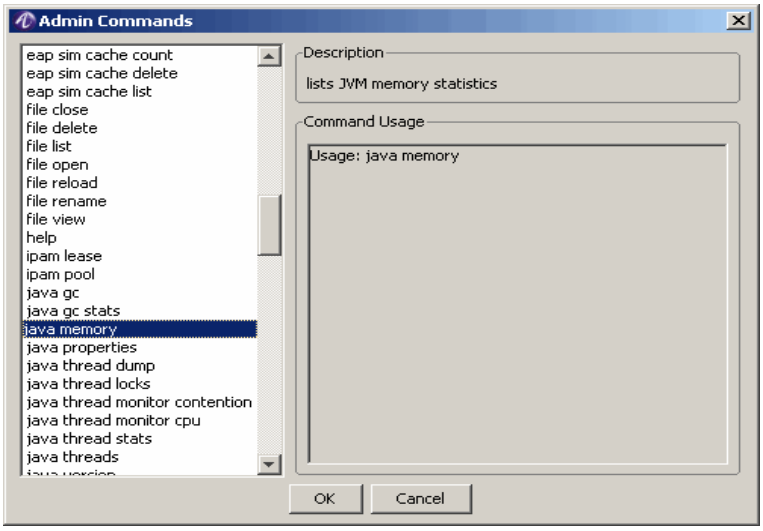
This screen allows the user to execute arbitrary administrator interface commands. The commands are defined in a text field in the top section of the work area and then are sent to the server for execution. Commands may be directly typed into the text field or may be selected from the Admin Commands window as shown in Figure 18-12.

To display the Admin Commands window, click the **...** that is on the right side of the text field. The Admin commands window is displayed, as shown in Figure 18-12.

After selecting a command from the list in the Admin Commands window, command usage or information appears in the right side pane of this window. Click **OK** to accept the displayed command. The command appears in the Commands window text field. Type any additional parameters that are required and then click the arrow at the right of the text field or press the enter key.

Command execution output is displayed in the lower work area window.

Figure 18-12 LiveAdministrator-Admin Commands



There are two buttons at the bottom of the Commands window of Figure 18-11.

The **Clear** button removes all information from the text area window.

The **History** button displays a pop-up window (Figure 18-13) containing commands that have been entered through this interface. To execute a command line again, select it and press the **Select** button. It is automatically executed.

Figure 18-13 LiveAdministrator-History Select Commands

END OF STEPS

Part V: File Tools Navigation Pane

Overview

Purpose

This part consolidates the chapters related to File Tools in the SMT Navigation pane.

Contents

This part includes the following chapters.

19 Creating and Managing User Profiles with Files

Overview

Purpose

A user profile is a set of information about a user. This information is used to authenticate the user and authorize access to services. In 8950 AAA this information minimally consists of a User-Name and Password and in many cases some sort of information indicating the type of service the user is supposed to receive is included. More traditional RADIUS servers often include verification attributes (often referred to as *Check-Items*) and reply attributes (often referred to as *Reply-Items*) in the user profile. However, in 8950 AAA this is usually done with *Attribute Sets*. The information used in 8950 AAA for authentication and authorization may come from a single source or may contain data collected from several sources combined together to form a single logical user profile.

The SMT provides two means for managing user profiles: standard RADIUS user files (text-based) and a built-in database. This chapter covers the use of the Server Management Tool (SMT) to manage standard text-based RADIUS user files.

The User File panel allows you to create and edit create user files and to create and maintain profiles for individual users in those files.

The following topics, included in this chapter, show how to create a user file and add and edit user profiles.

The User File

User file

A 8950 AAA user file is a text file that contains user profiles for users authorized to access your network.

A user file contains one or more profile entries. Each entry is indexed by an index key. The User-Name is typically used as the index key, but it is also possible to create entries indexed by other data: real name, DNIS (Dialed Number), Realm, etc. Profiles with user names as the index key are commonly referred to as *user profiles* while entries indexed by some other attribute are often referred to as *attributes sets*.

In 8950 AAA, all user files are stored in the 8950 AAA run directory.

The PolicyAssistant and User Files

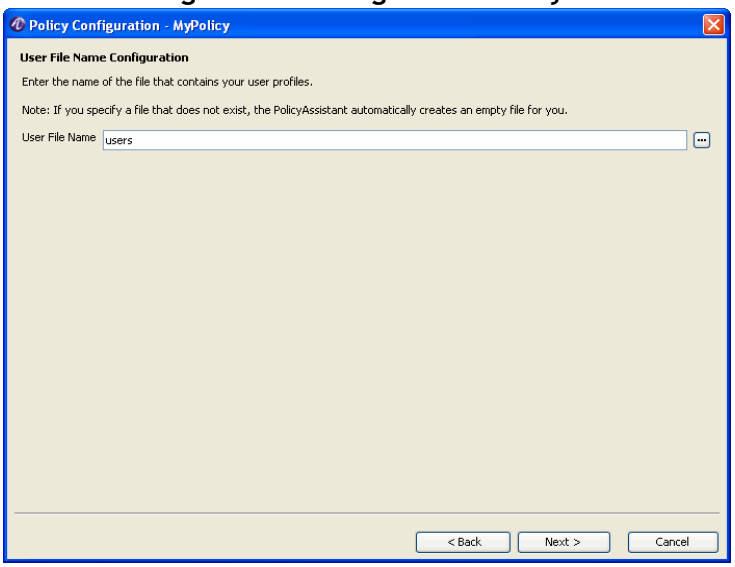
User files and Policy Assistant

When using the PolicyAssistant, a user file can be specified as the User Profile Source for a policy.

When using the PolicyAssistant, if a RADIUS User File is selected as the User Profile Source, the PolicyAssistant requires the name of the user file. The file name is entered using the dialog box shown in Figure 19-1.

Important! A user file can be used in more than one policy.

Figure 19-1 User File Configuration Dialog in the PolicyAssistant



If the file you named does not exist, then the PolicyAssistant will create an empty file for you. In addition to creating a new user file, PolicyAssistant can also create and maintain user files through the SMT User Files panel. This is addressed in the next section.

The SMT User Files Panel

SMT User Files Panel

The SMT User Files panel allows you to access and create user files and to create and maintain profiles for individual users. The following steps illustrate how to create and edit user files with the SMT:

- Opening an Existing User File
- Creating a New User File
- Adding a New User
- Setting Verification Attributes for a User
- Setting Reply Attributes for a User
- Adding Comments About a User
- Completing the User Profile

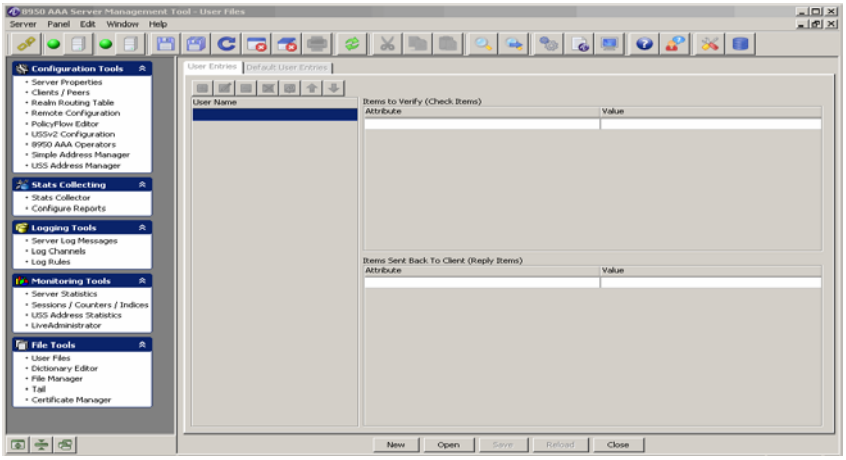
The following sections list the steps necessary to perform each of the procedures associated with user profiles and user files.

Opening an Existing User File

Use the following procedure to access and display information about an existing user file.

1. Select **User Files** from the **File Tools** folder on the Navigation pane. The User Files panel appears as shown in Figure 19-2.

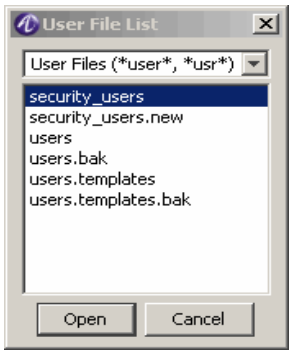
Figure 19-2 The User Files panel



Important! Note that the panel title is simply *User Files* and no file name is listed; when the User Files panel is first opened, no user file is loaded.

2. If you have defined a user file using the PolicyAssistant, then that file will be listed. Click **Open**. The User File List box appears as shown in Figure 19-3.

Figure 19-3 User File List Box



3. Select the user file to load and click **Open**.

Result: Information about the open file is displayed within the User Files panel. The User Files panel now shows the details of the selected user file, as shown in Figure 19-4.

Figure 19-4 The User Files panel

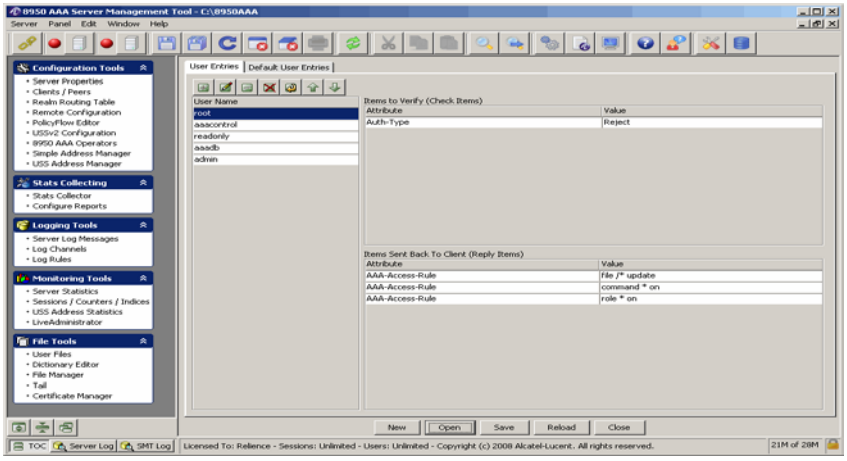
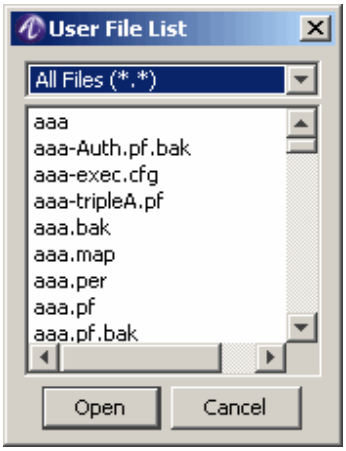


Figure 19-5 User File List: List All Files



Important! The SMT identifies a file as a user file if it is located in the run directory and the file name contains either *users* or *usr*. To list all files in the run directory, click the drop list (at the top of the box) and select All Files (*.*) as illustrated in Figure 19-5.

If you have standard RADIUS formatted user files that you have created using other tools, copy the files to the run directory. Make sure they file names contains “usr” or “user” so you can easily access the files from the User Files Panel.

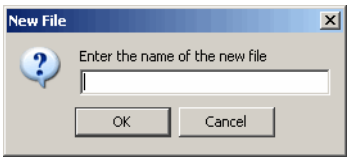
Creating a New User File

The following procedure shows how to create a user file:

1. Select **New** on the User Files panel.

   Result: The New File dialog appears, as shown in Figure 19-6.

Figure 19-6 New User File Dialog



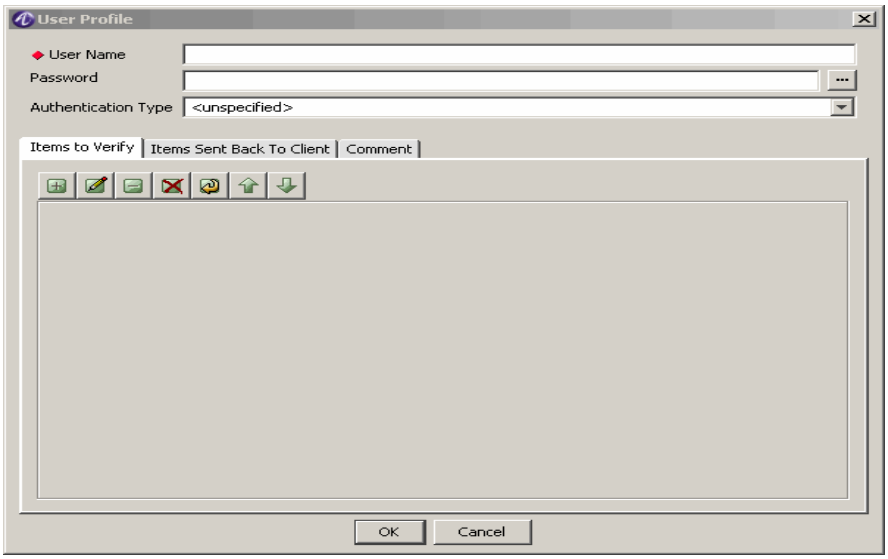
2. Enter a name for the new user file in the New File dialog.
3. Click **OK** to return to the User Files panel and load the selected file.

Adding a New User

The following procedure describes how to add a new user to a user file:

1. From the User Files panel, click the **Insert a record** button to create a new user profile. The User Profile dialog appears as shown in Figure 19-7.

Figure 19-7 New User Profile Dialog



2. Enter the **User Name** for this profile.

   You must enter the user's name exactly as the user will enter it when logging on to your network.

   If you use realms on your network, you would not normally enter the realm as part of the user name in this dialog. For example, if User1 enters user1@myisp.com in a remote access dialog, enter the user name as `user1`. If your network has multiple realms you should create a separate user file for each realm.

3. Enter the user's plain text **Password**.

   You must enter the user's password exactly as the user enters it when logging on to your network.

   Important! Make sure you use the correct case.

`SeCrEt` *is not the same as* `secret`.

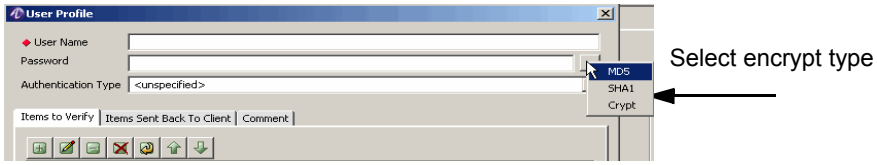
4. As an option, you may *hash* the password for storage. Click the ... next to the password field. Select an hash type from the list that appears, as shown in Figure 19-8.

   Important! We use the term “hash” instead of “encryption” because the process of hashing cannot be reversed. By definition, something that can be encrypted can also be decrypted. For authentication checking of hashed passwords, 8950 AAA takes the password entered by the user and hashes it using the exact same calculation that was used to hash the password in the user profile.

   If the two resulting hashes match, then the two passwords must have been the same.

   Note that use of hashed passwords in a user’s profile requires the use of the PAP (Password Authentication Protocol) in the PPP session. CHAP (Challenge Handshake Authentication Protocol) cannot be used with hashed password in the user profile.

Figure 19-8 User Profile Dialog-Password hash Type



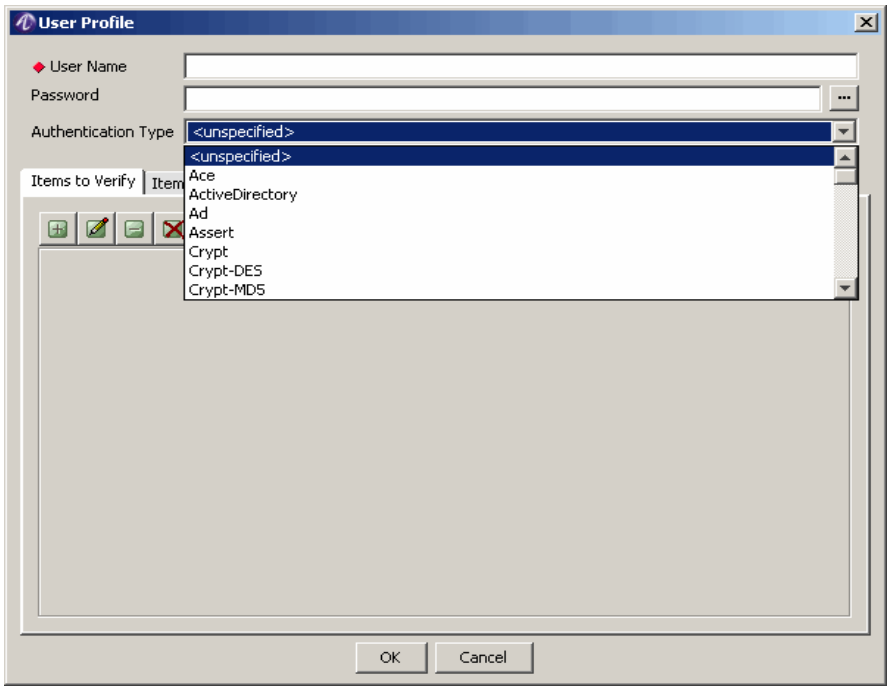
   The plain text password is replaced by the encrypted password. For example, if you enter “MySecretPassword” and select MD5 encryption, the Password field now contains something like:

   $MD5$3XzCR7LP$fJ7/npaleWkxnfWQjWidiO

   Important! The results will be different each time you perform the hash. Do not attempt to hash a password that has already been hashed. The resulting value is unusable and the hash process cannot be undone.

5. As an option, specify the **Authentication Type** from the drop-down list, as shown in Figure 19-9.

Figure 19-9 User Files-List of Authentication Types



Important! This field is only available in Expert mode. If you are not in Expert mode, then the Authentication Type attribute, if set, is only visible under the Items to Verify tab (See Figure 19-4).

The Authentication Type is provided for backwards compatibility with user files imported from older RADIUS servers. If you set password hashing in Step 4 above, the Authentication Type is preset for you—do not change it.

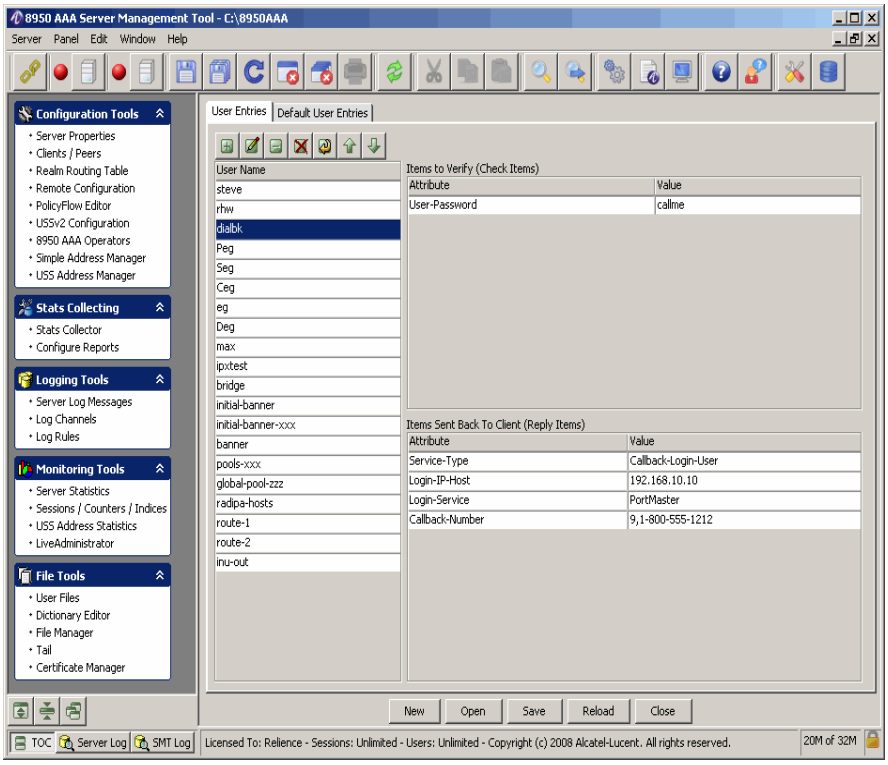
Important! Setting the Authentication type is not recommended when using the PolicyAssistant.

Opening an Existing User Profile

The following procedure explains how to open a user profile from within a user file.

1. Open a user file as described in "Opening an Existing User File" on page 3.
2. Select the User Profiles tab to display the list of User Names associated with this User File as shown in Figure 19-10.

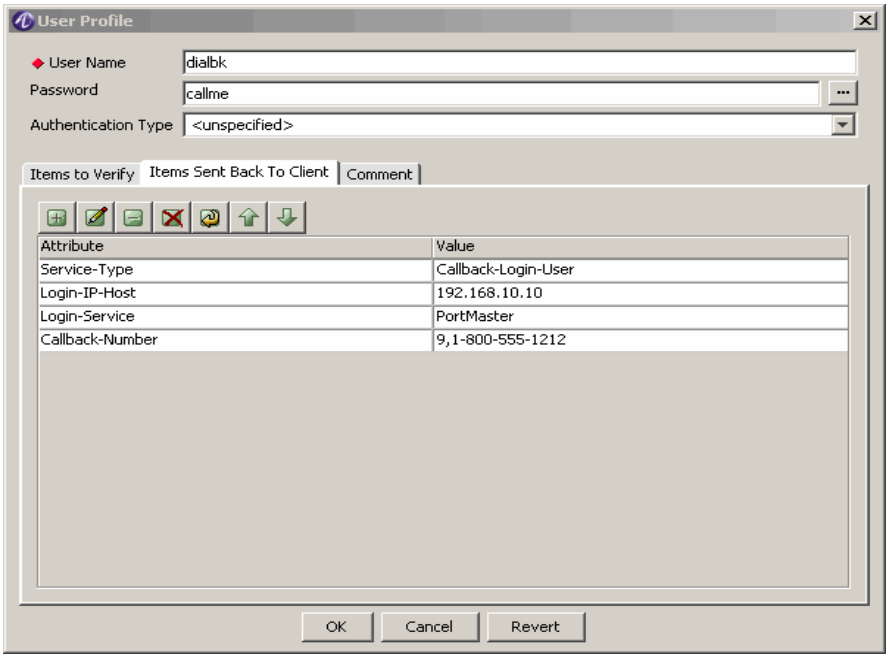
Figure 19-10 User Files-List of User Names



3. Double-click the user name that corresponds to the desired User Profile.

   Result: The User Profile window appears as shown in Figure 19-11.

Figure 19-11 User Profile



Setting Verification Attributes for a User

You may assign verification attributes to a user's profile to allow the server to perform additional authorization checks unique to this user. When using the PolicyAssistant this is normally not necessary.

If you use the PolicyAssistant to create policies, you can assign an *attribute set* that can provide the same functionality as verification attributes. If a conflict occurs, the attributes in the user's profile take precedence over the attribute set defined for the policy.

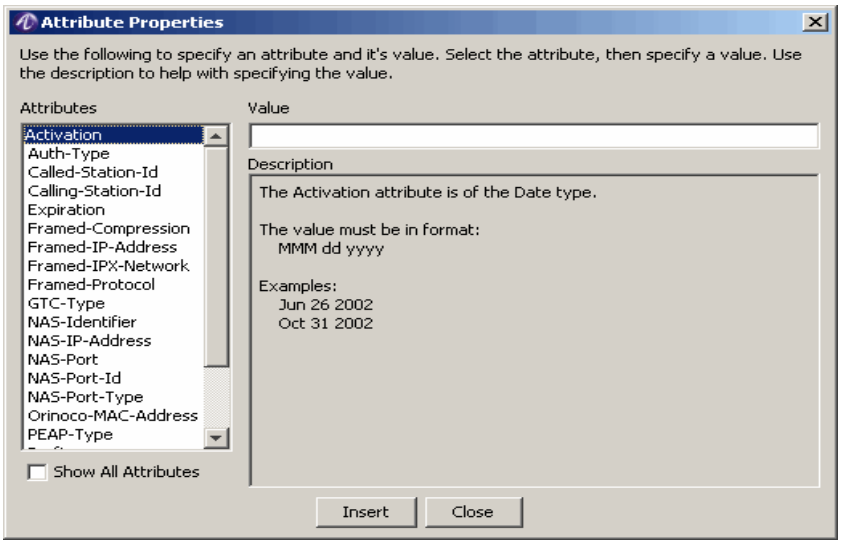
An attribute set provides a list of attributes that you can use for all users using the same policy. For example, if all your users must dial the same access number you must enter the *Called-Station-Id* attribute in all your user profiles. However, if you create an attribute set with this attribute and other common attributes, you only need to enter this once.

Attribute sets also provide a single point for updates. Instead of editing all your user profiles when the area code changes, you can change it once in the attribute set.

Use the following procedure to set verification attributes:

1. From the User Files window, open an existing user profile or create a new user profile, as described previously.
2. From the User Profiles window, click the **Items to Verify** tab to add verification attributes for this user.
3. Click the **Insert a record** button to open the Attribute Properties dialog as shown in Figure 19-12.

Figure 19-12 Attribute Properties Dialog



4. Select an attribute from the **Attributes** list. Depending upon the chosen attribute, the Value field will either be a text field or a drop-down list of possible values.
5. Type or select an appropriate value in the **Value** field and enter the value by clicking **Insert** or by pressing the Enter key.

   For example, if your users can only dial the `650-555-1212` access number, select the *Called-Station-Id* attribute and enter `6505551212` in the Value field.

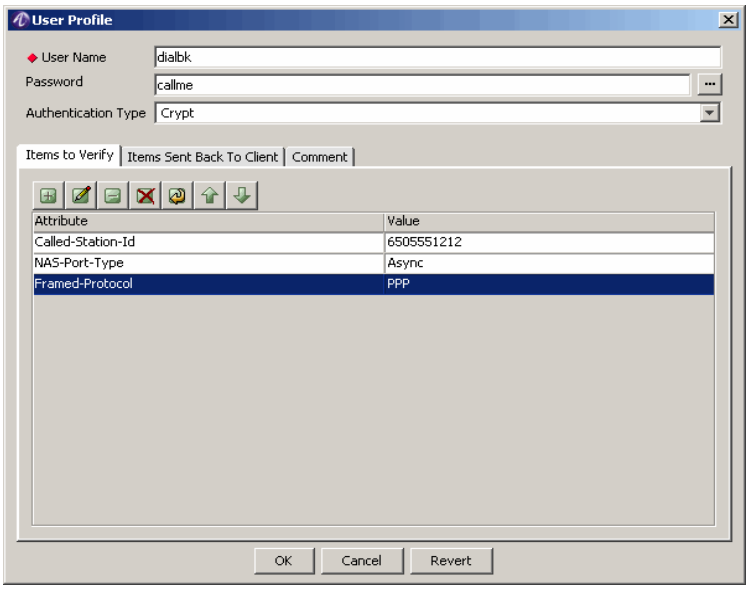
   Important! When entering telephone numbers, the format must match the format used by your local telephone company to send the information to your NAS.

   The Description field, which is below the Value field, provides guidelines on the format for those attributes that support arbitrary data entered from the keyboard.

   As an option, click **Show All Attributes** to display all attributes included within the dictionary selected in the server profile.

   Important! To change the attributes that appear in this list, select Preferences from the Edit menu. Select the Check Items List option from the Server Management Tool Preferences dialog.
6. Repeat Step 4 and Step 5 to enter multiple attributes while the attribute properties window is open.
7. Click **Close** to close the Attribute Properties dialog and return to the User Profile dialog. The verification attributes that were specified display on the Items to Verify tab as shown in Figure 19-13.

Figure 19-13 User Profile Dialog-Items to Verify tab



Setting Reply Attributes for a User

Set reply attributes to enable the NAS to configure the session for this user. The server returns these attributes to the NAS if the authentication step is successful. This is referred to as *session provisioning*.

You may assign reply attributes to a user's profile and 8950 AAA will return these attributes to the NAS if the authentication and authorization steps are successful. This is referred to as *session provisioning*. When using the PolicyAssistant this is normally not necessary.

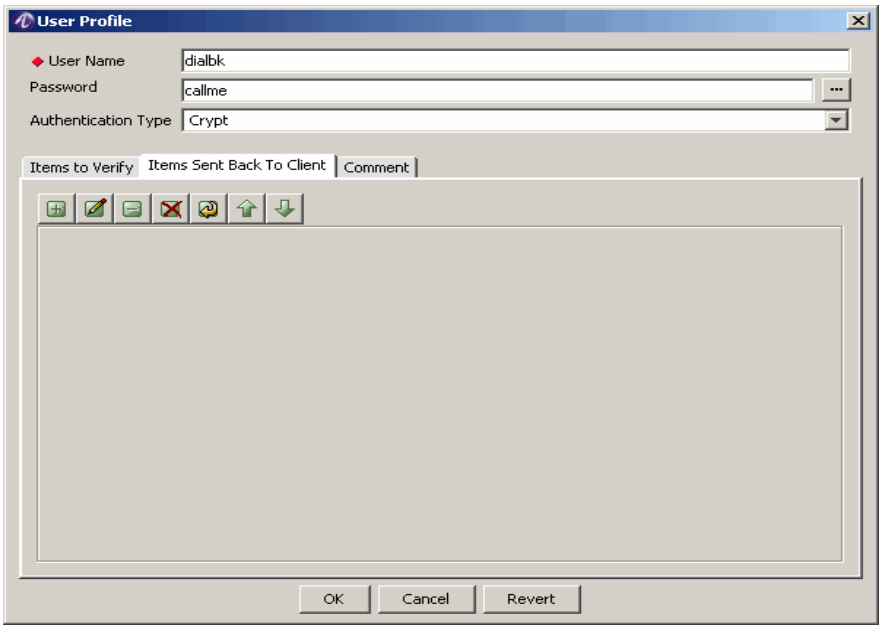
If you use the PolicyAssistant to create policies, you can assign an *attribute set* that can provide the same functionality as reply attributes. If a conflict occurs, the attributes in the user's profile take precedence over the attribute set defined for the policy.

An attribute set provides a list of attributes that you can use for all users using the same policy. For example in Step 3 on page 10, if all your users are restricted to using PPP then you would have to enter *Framed-Protocol=PPP* in every user's profile. However, if you create an attribute set with this attribute and other common attributes, you only need to enter this once.
Attribute sets also provide a single point for updates. Instead of editing all your user profiles when the area code changes, you can change it once in the attribute set.

The following procedure lists the steps for setting reply attributes:

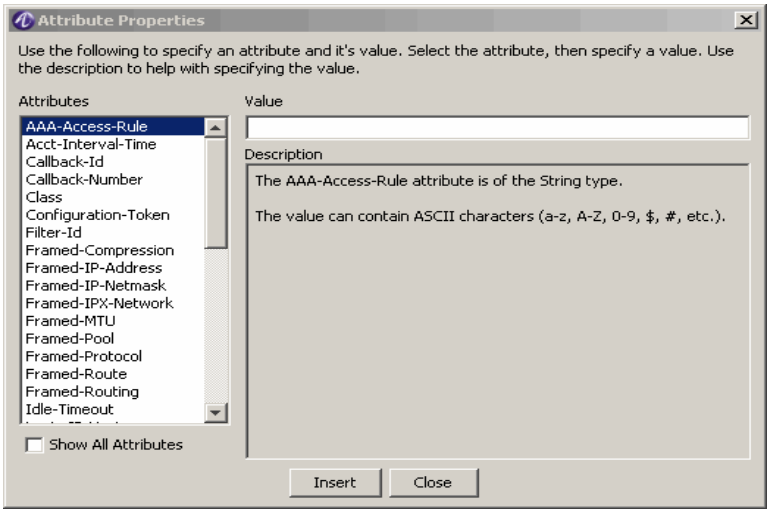
1. From the User Profiles window, click the **Items Sent Back to Client** tab to add reply attributes for this user as depicted in Figure 19-14.

Figure 19-14 User Profile–Items Sent back to NAS



2. Click **Insert a record** to open the Attribute Properties dialog as shown in Figure 19-15.

Figure 19-15 Attribute Properties



3. Select an attribute from the **Attributes** list. Depending upon the chosen attribute, the Value field will either be a text field or a drop-down list of possible values.

4. Type or select an appropriate value in the **Value** field and enter the value by clicking **Insert** or by pressing the Enter key.

   For example, you can limit the session time to one hour, select the *Session-Timeout* attribute and enter `3600` in the Value field; or on a Alcatel-Lucent NAS product to identify a specific IP address pool from which addresses are assigned, select the *Ascend-Assign-IP-Pool* attribute and enter an appropriate value in the Value field.

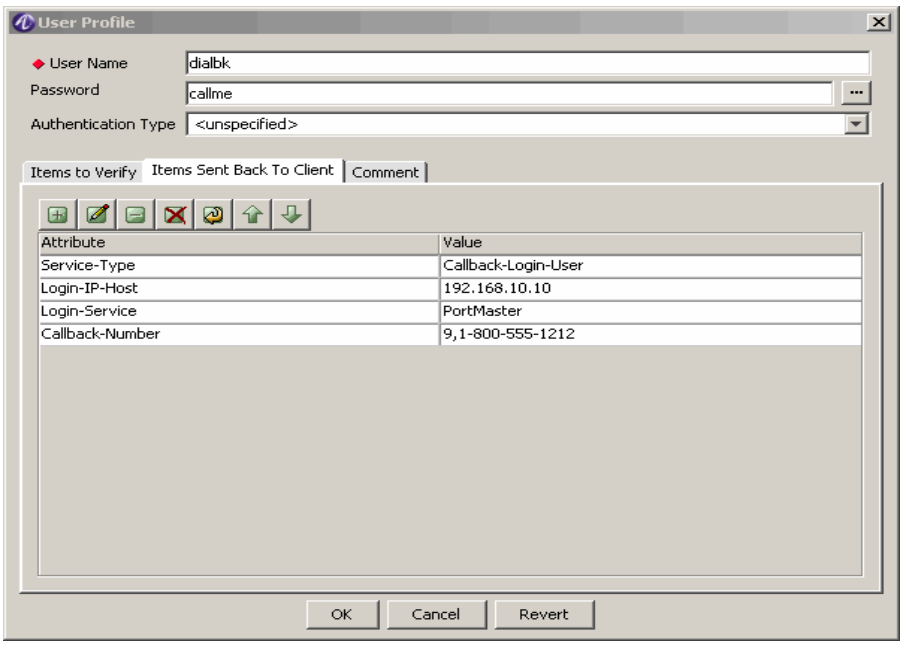
   The Description below the Value field, provides guidelines on the format for those attributes that support arbitrary data entered from the keyboard.

   Select the **Show All Attributes** checkbox to display all attributes included within the dictionary selected in the server profile.

   Important! To change the attributes that appear in this list, select Preferences from the Edit menu. Select the Reply Items List option from the Server Management Tool Preferences dialog.

5. Repeat Step 3 and Step 4 to enter multiple attributes while the attribute properties window is open.
6. Click **Close** to close the Attribute Properties dialog and return to the User Profile dialog. The reply attributes that were specified appear on the Items Sent Back to Client tab as shown in Figure 19-16.

Figure 19-16 Attribute Properties-Reply Items



Adding Comments About a User

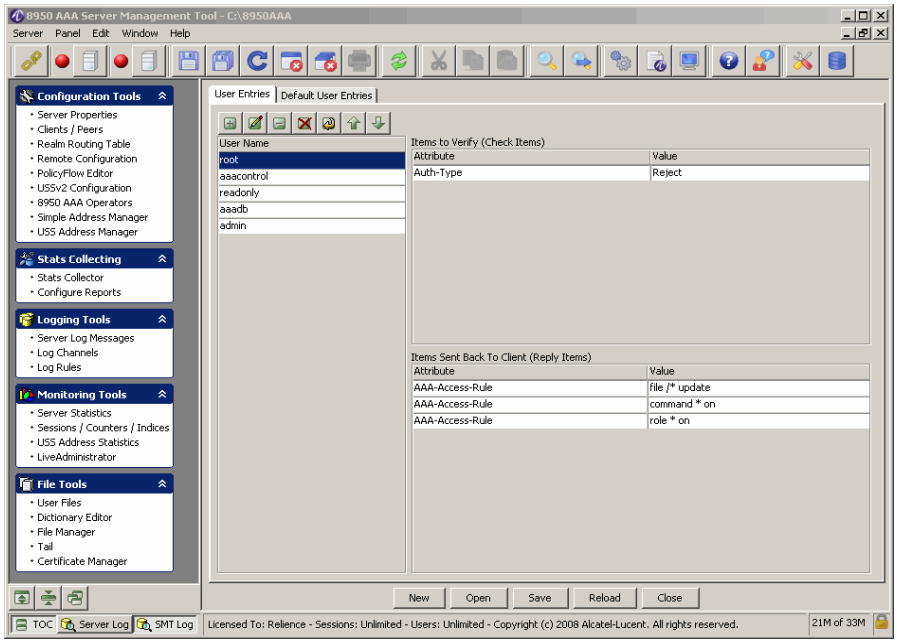
You may add comments about a user on the *Comment* tab. Any comments you enter are added to the user file. Use this tool to document user files or save information about a user that cannot be stored elsewhere.

Completing the User Profile

The user file shown in Figure 19-13 indicates that the server will only authorize user Userxyz if he dials `650-555-1212` while using an Asynchronous line (not ISDN) and PPP. If the server authenticates and authorizes Userxyz, it sends an instruction to the NAS to assign the user session an IP address from pool 1 (address pools must be configured on the NAS) and the session is limited in length to one hour.

Click **OK** to close this dialog and return to the User Files panel.

Figure 19-17 User Profile Panel-with selected user profile



Saving Changes to the User Profile

To make any changes to the file permanent, click **Save** on the Clients panel.

To make changes to the currently running 8950 AAA server, you must click **Reload** on the User Files panel.

Important! From the procedures that are described above, it is important to be able to run the following for each user that is added:

- Adding a New User
- Opening an Existing User Profile
- Setting Verification Attributes for a User
- Setting Reply Attributes for a User
- Adding Comments About a User
- Completing the User Profile

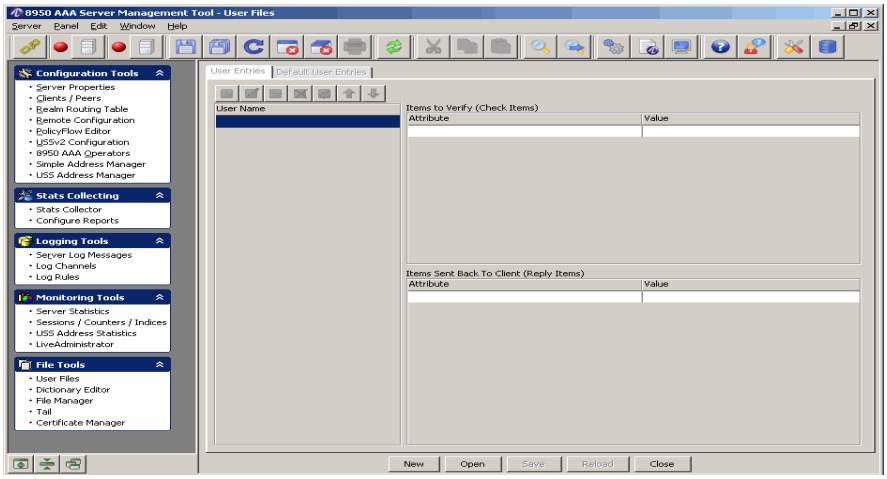
Creating an Attribute Set File

Attribute Sets

Attribute Sets are stored in RADIUS user files called *users.templates*. Attribute sets are also frequently called *templates*. The following procedure shows how to create a user file and add an attribute set to it. An attribute set is virtually the same as a user profile. The only difference is that the index key for an attribute set is normally a real name of other functional descriptor rather than being a User-Name.

1. Select **User Files** from the **File Tools** folder on the Navigation pane. The User Files panel appears as depicted in Figure 19-18.

Figure 19-18 SMT Navigation Pane and an empty User Files panel



Note that the panel title is simply User Files and no file name is listed; when the User Files panel is first opened, no user file is loaded.

1. Click **New** to create a new file and enter a name for your attribute set file. The New File Dialog, as shown in Figure 19-6 is displayed.
2. Enter a name for the new user file in the New File dialog.
3. Click **OK** to return to the User Files panel and load the selected file.
4. Click **Close** to close the User Files panel. Use the Policy Wizard under the PolicyAssistant panel to add attribute sets to your new *template* file.
5. Click the **Insert a record** button to open the User Profiles panel. Click the **Insert a record** button to open Attribute Properties dialogue. Enter the attributes and click **Insert.**

END OF STEPS

20 8950 AAA Dictionary Editor

Overview

Purpose

This section provides information about the 8950 AAA Data Dictionary and some of the terms that you will encounter when working with the 8950 AAA product.

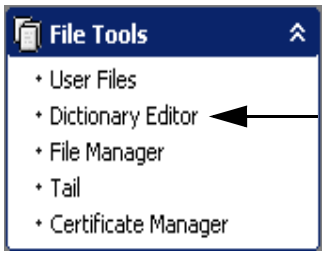
The following topics are included in this chapter:

Accessing the Dictionary Editor Panel

About accessing the Dictionary Editor

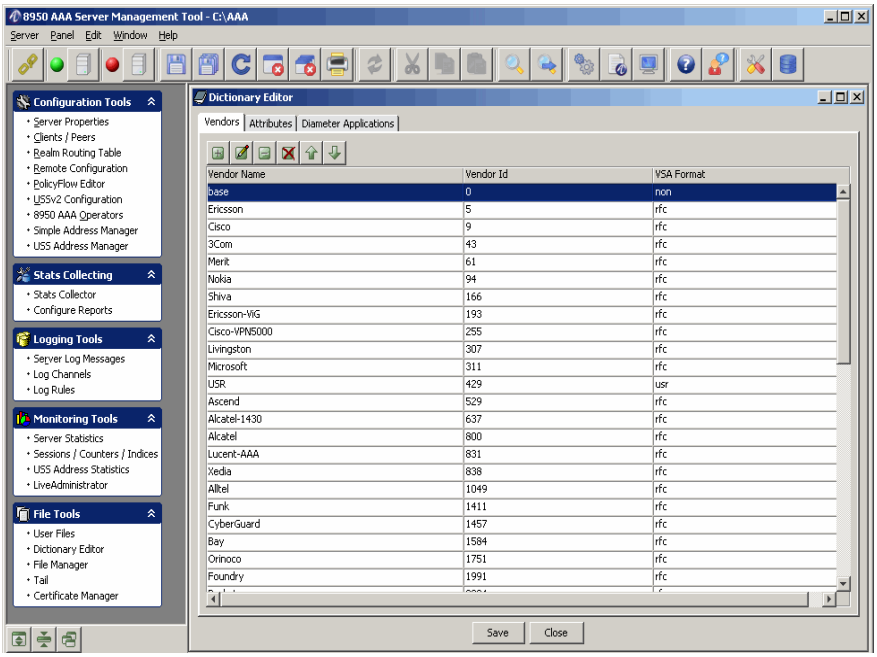
Using the SMT, select **Dictionary Editor** under **File Tools**, from within the Navigation Pane, as shown in Figure 20-1.

Figure 20-1 Navigation Pane-Dictionary Editor



The Dictionary Editor panel appears as shown in Figure 20-2.

Figure 20-2 8950 AAA Dictionary Editor Panel



The Dictionary Editor Panel

Use the Dictionary Editor panel to manage information about the Vendors, Attributes, and Diameter Applications of 8950 AAA.

By default, the details of the Vendors tab is displayed when the Dictionary Editor panel is opened.

The Dictionary Editor panel contains 3 tabs, as follows:

- Vendors
- Attributes
- Diameter Applications

Each of these tabs allow you to manage different types of attributes of the Dictionary Editor.

Vendors Tab

About the Vendors tab

The Vendors tab allows you to configure and manage the attributes related to vendors in the 8950 AAA.

By default when you click on the Dictionary Editor panel, the Vendors tab is displayed, as shown in Figure 20-2.

Table 20-1 explains the attributes of the Vendors tab.

Table 20-1 Dictionary Editor-Vendors tab properties

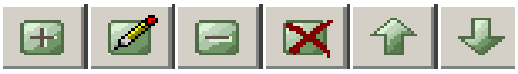
Properties	Description
Vendor Name	The name of the Vendor.
Vendor ID	The Vendor Identification code or number.
VSA format	The Vendor Specific Attribute (VSA) format.

Using the Vendors tab Action buttons

The **Vendors** tab panel also consists of a set of Action Buttons that appear at the top of the 8950 AAA Dictionary Editor's Vendors tab panel, as shown in Figure 20-2.

The Vendors tab action buttons are as shown in Figure 20-3.

Figure 20-3 Vendors tab-Action buttons



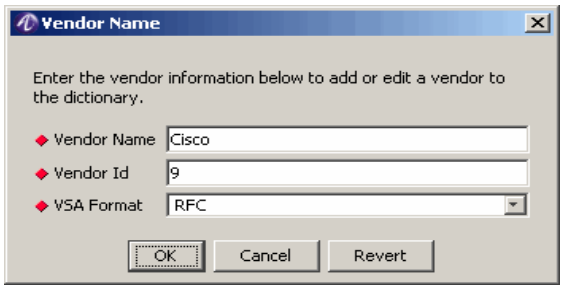
These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

1. The **Insert a record** action button displays the Vendor Name dialog panel, as shown in Figure 20-4. This panel allows you to add a vendor information to the dictionary.

Figure 20-4 Dictionary Editor-Vendor Name Dialog



2. The **Edit a selected record** action button displays the Vendor Name dialog panel, as shown in Figure 20-4. This displays the selected Vendor information and allows you to edit the vendor information in the dictionary.
3. The **Delete selected record** action button allows you to delete the selected vendor information.
4. The **Delete all records** action button allows you to delete all the vendor records.
5. The **Move selected record up** action button allows you to move the selected record up.
6. The **Move selected record down** action button allows you to move the selected record down.

Attributes Tab

About the Attributes tab

The Attributes tab allows you to configure and manage the attributes related to a vendor in the 8950 AAA.

To go to the Attributes tab, click on the Attributes tab in the Dictionary Editor panel. The details about the Attributes tab dialog or panel are displayed, as shown in Figure 20-5.

Figure 20-5 Dictionary Editor Panel-Attribute tab properties

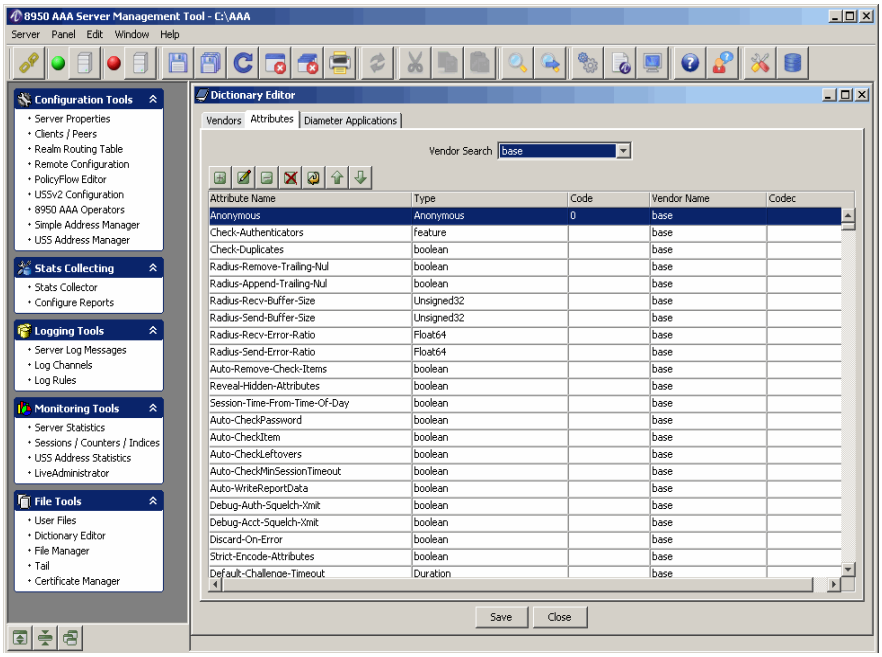


Table 20-2 explains some of the properties in the Attributes tab.

Table 20-2 Dictionary Editor-Attributes tab properties

Properties	Description
Vendor Search	Select a vendor name who is providing the service. The Attributes properties are sorted and displayed according to the selected Vendor.
Attribute Name	The name of the Attribute.
Type	The type of the Attribute.
Code	The Attribute Code.
Vendor Name	The name of the Vendor.
Codec	The code encode and decoder.

Using the Attributes tab Action buttons

The **Attributes** tab panel also consists of a set of Action Buttons that appear at the top of the 8950 AAA Dictionary Editor's Attributes tab panel, as shown in Figure 20-5.

The Attributes tab action buttons are as shown in Figure 20-6.

Figure 20-6 Attributes tab-Action buttons

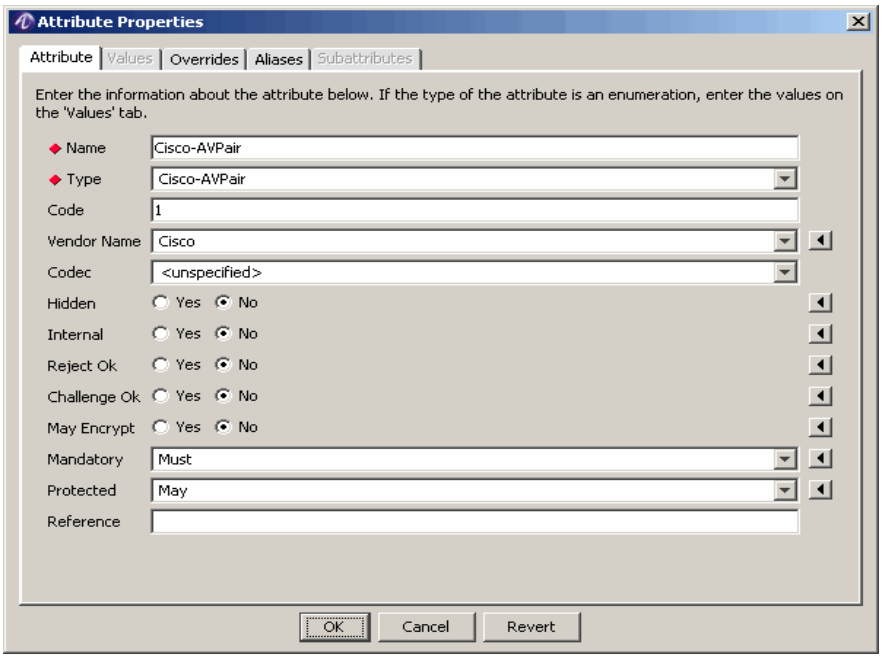
These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

1. The **Insert a record** action button displays the Attribute Properties dialog, as shown in Figure 20-7. This dialog allows you to add attribute information to the dictionary.

Figure 20-7 Dictionary Editor Panel-Attribute properties dialog



The Attribute Properties dialog has a set of tabs namely, Attribute, Values, Overrides, Aliases, and Subattributes.

The Attribute tab is the default tab.

Table 20-2 explains the attributes of the Attribute panel

Table 20-3 Dictionary Editor-Attributes of Attributes tab

Attributes	Description
Name	Name of the Attribute to be created.
Type	Type of the Attribute.
Code	The Attribute code.
Vendor Name	Name of the Vendor.
Codec	The code encode and decoder.
Hidden	If set true, the attribute value is not displayed in the Server Log file or Accounting Log file.
Internal	Attributes whose code is greater than 255. Used internally within radius sever and is not be sent to NAS

Table 20-3 Dictionary Editor-Attributes of Attributes tab

Attributes	Description
Reject Ok	During radius reject disposition processing, if an attribute in the reply variable group is not marked reply-ok = true, then it is not included in the Access-Reject.
Challenge Ok	During radius challenge disposition processing, if an attribute in the reply variable group is not marked challenge-ok = true, then it is not included in the Access-Challenge.
May Encrypt	If enabled, code is encrypted.
Mandatory	A flag rule. Used for recording diameter M-bit rules.
Protected	Not used.
Reference	A comment field to record which specification defined the AVP/value/command.

The Values tab allows you to enter the list of values for the attribute. The Value text replaces the Code value when printed in log files and accounting records. Code must be unique to values for this attribute.

Use Subattributes tab to add the subattributes of the attributes selected provided it has the subattributes.

Important! Values are only valid with types of enumeration and tagged-enumeration.

Separate multiple Aliases with a comma.

The Overrides tab allows you to enter the codec overrides for the attribute.

The Aliases tab allows you to enter the aliases for the attribute. Some vendors use different attribute names that have the same functionality as default attributes. These are called Aliases.

2. The **Edit a selected record** action button displays the Attribute Properties dialog, as shown in Figure 20-7. This displays the selected Attribute's information and allows you to edit the attribute information in the dictionary.
3. The **Delete selected record** action button allows you to delete the selected attribute information.
4. The **Delete all records** action button allows you to delete all the attribute information.
5. The **Make a copy of the selected record** action button allows you to copy the properties of the selected attribute information and save it as a different attribute.
6. The **Move selected record up** action button allows you to move the selected record up.

7. The **Move selected record down** action button allows you to move the selected record down.

Diameter Applications Tab

About the Diameter Applications tab

The Diameter Applications tab allows you to configure and manage the diameter application details related to a vendor in 8950 AAA.

To go to the Diameter Applications tab, click on the Diameter Applications tab in the Dictionary Editor panel. The details about the Diameter Applications dialog or panel is displayed, as shown in Figure 20-8.

Figure 20-8 Dictionary Editor Panel-Diameter Applications properties

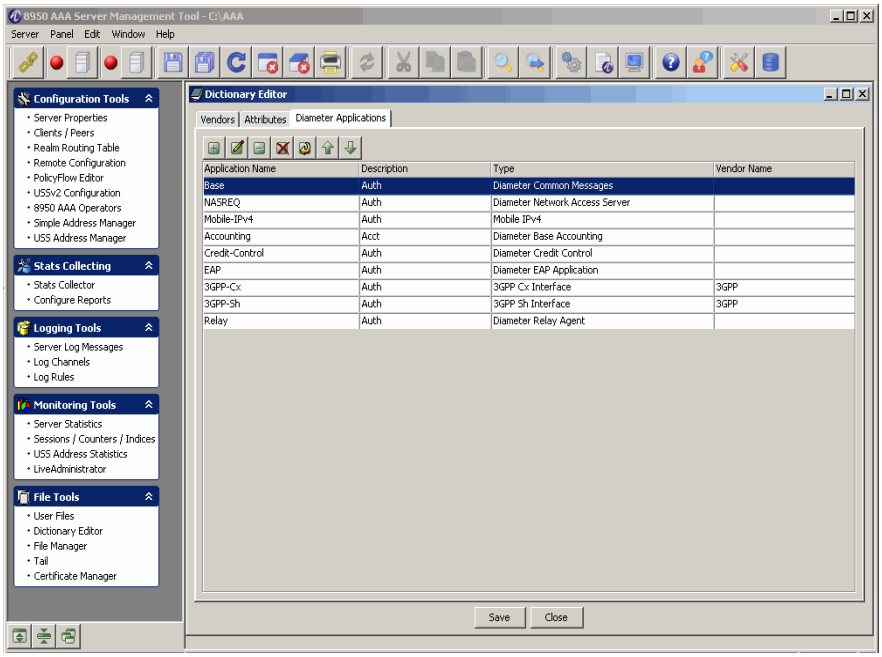


Table 20-4 explains the properties in the Diameter Applications tab.

Table 20-4 Dictionary Editor-Diameter Applications tab properties

Properties	Description
Application Name	The name of the application.
Description	The description about the diameter application.
Type	The type of the application.
Vendor Name	The name of the Vendor.

Using the Diameter Applications tab Action buttons

The **Diameter Applications** tab panel also consists of a set of Action Buttons that appear at the top of the 8950 AAA Dictionary Editor's Diameter Applications tab panel, as shown in Figure 20-8.

The Diameter Applications tab action buttons are as shown in Figure 20-9.

Figure 20-9 Diameter Applications tab-Action buttons

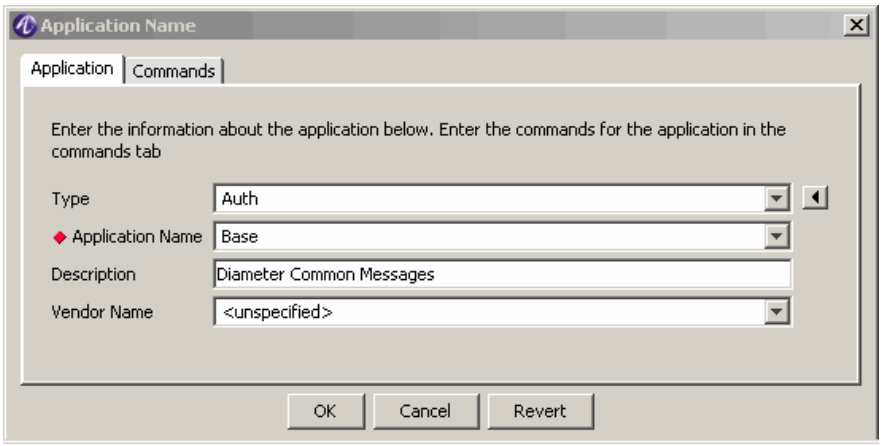
These action buttons allow you to perform the following actions:

- Insert a record
- Edit selected record
- Delete selected record
- Delete all records
- Make a copy of selected record
- Move selected record up
- Move selected record down

You can perform any of the required actions using these action buttons.

1. The **Insert a record** action button displays the Application Name dialog, as shown in Figure 20-10. This dialog allows you to add the diameter application information to the dictionary.

Figure 20-10 Dictionary Editor Panel-Application Name dialog



The Application Name dialog has two tabs namely, Application tab and commands tab.

The Application tab is the default tab that allows you to enter the application details.

The Commands tab allows you to enter the commands for the application.

2. The **Edit a selected record** action button displays the Application Name dialog, as shown in Figure 20-10. This displays the selected Application information and allows you to edit the application information in the dictionary.
3. The **Delete selected record** action button allows you to delete the selected application information.
4. The **Delete all records** action button allows you to delete all the application information.
5. The **Make a copy of the selected record** action button allows you to copy the properties of the selected application information and save it as a different application.
6. The **Move selected record up** action button allows you to move the selected record up.
7. The **Move selected record down** action button allows you to move the selected record down.

END OF STEPS

21 Managing files

Overview

Purpose

This section discusses 8950 AAA files and how to create and manage them using the File manager panel.

The following topics are included in this chapter:

The File Manager Panel

File manager panel

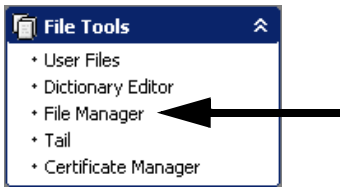
The File Manager panel enables the user to perform a variety of operations on 8950 AAA files. These operations include:

- Create a new file.
- Copy the contents of an existing file to a new file
- Edit the contents of a file
- Rename an existing file
- Delete a file

All file operations are limited to the 8950 AAA run directory.

To display the File Manager panel, select **File Manager** from the Navigation Pane, under **File Tools**, as shown in Figure 21-1.

Table 21-1 Navigation Pane-File Manager



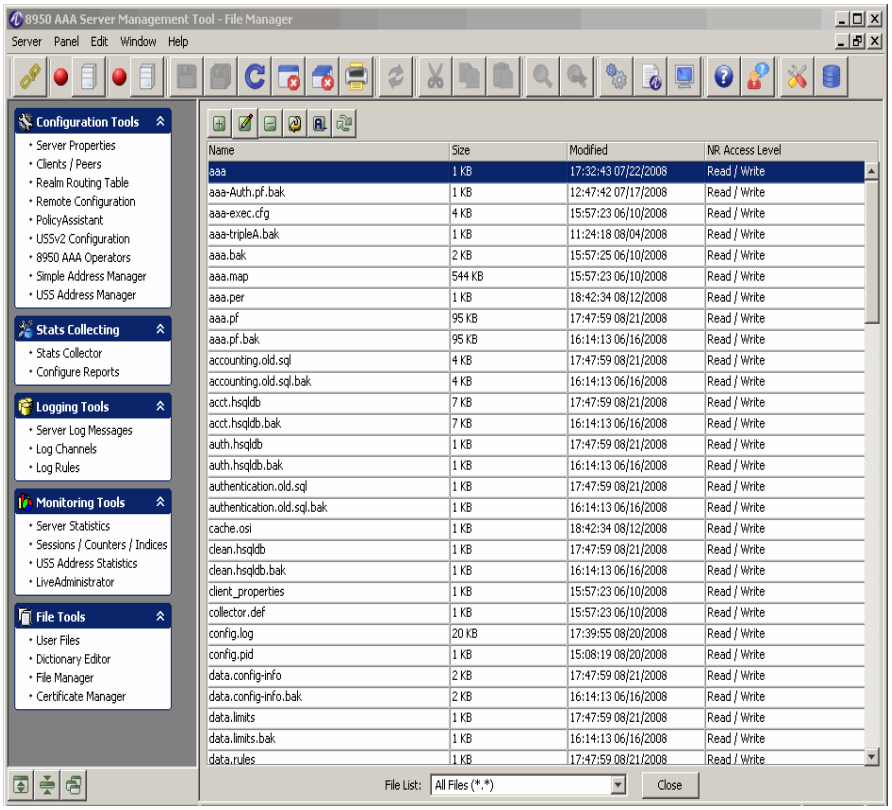
Viewing File Attributes and File Content

As shown in Figure 21-1, the File Manager panel displays the following attributes of a file:

- Filename
- File size
- Date last modified
- NR Access Level

Select the desired files to be displayed in the File Manager panel, from the File List drop-down list.

Figure 21-1 File Manager Panel



There are many different types of files that are used by 8950 AAA File Manager. The most commonly used files that would be of interest to an admin user are listed in Table 21-2.

Table 21-2 Configuration Files

File Name	File Description
acct_methods*	The PolicyFlow to be executed for processing accounting requests. You may also use the PolicyFlow editor in the SMT to manage this data.
auth.pf*	The PolicyFlow to be executed for processing authentication requests.You may also use the PolicyFlow editor in the SMT to manage this data.
client_properties	Information about client classes and is used to set per-client specific information. Use the clients panel in the SMT to manage this data.
data.config-info*	Data file used by the PolicyAssistant.

Table 21-2 Configuration Files

File Name	File Description
data.dnis-info.csv*	Data file used by the PolicyAssistant.
data.realm-info.csv*	Data file used by the PolicyAssistant.
db_properties	Settings for the internal database.
dictionary.ser	A serialized version of the XML dictionary file. Do not edit this file.
dictionary.xml	The 8950 AAA Dictionary in XML format. The SMT provides a GUI Dictionary editor which is available when running in *Expert Mode*.
licence.txt	The 8950 AAA license file. DO NOT EDIT THIS FILE.
log_channels	Definitions of available log channels. A GUI editor is available in the SMT for managing this data. You may also use the Log Channel in SMT to manage this data.
log_rules	Rules controlling log operations. A GUI editor is available in the SMT for managing this data. You may also use the Log rule in SMT to manage this data.
method_dispatch*	Selects the initial method invoked for a RADIUS request. You may also use the PolicyFlow editor in the SMT to manage this data.
policy.log	The default log channel for 8950 AAA log messages.
policy.pid	The *Process ID* for the 8950 AAA process.
policyassistant_properties*	Various settings for the PolicyAssistant.
security_properties	Various settings for maintaining 8950 AAA system security. A GUI editor is available in the SMT for managing this data. You may also use the 8950 AAA Operators Panel in the SMT to manage this data.
security_users	A users file containing profiles for 8950 AAA admin users. A GUI editor is available in the SMT for managing this data. You may also use the 8950 AAA Operators Panel in the SMT to manage this data.

Table 21-2 Configuration Files

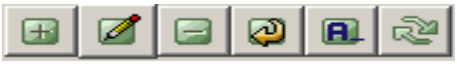
File Name	File Description
server_properties	Global server settings. A GUI editor is available in the SMT for managing this data. You may also use the 8950 AAA Server Properties Panel in the SMT to manage this data.
smt.log	Messages logged from the SMT application.
users	The default file containing user profiles. This file may not be used at your location. A GUI editor is available in the SMT for managing this data. You may also use the User File Editor in the SMT to manage this data.
users.templates	Templates (Attribute sets) for use in the PolicyAssistant and other PolicyFlow. When using the PolicyAssistant a GUI editor is available in the SMT for managing this data. You may also use the User File Editor in the SMT to manage this data.
uss_counters	Settings defining counters to be maintained by the Universal State Server (USS). You may also use the Server Properties Panel in the SMT to manage this data.
uss_indices	Settings defining indices to be maintained by the Universal State Server (USS). You may also use the Server Properties Panel in the SMT to manage this data.

Important! Files marked with an asterisk (*) should not be modified if you are using the PolicyAssistant.

Action buttons in the File Manager Panel

There are six action buttons at the top of the File Manager panel, as shown in Figure 21-2.

Figure 21-2 File Manager panel-Action buttons



These are described in Table 21-3.

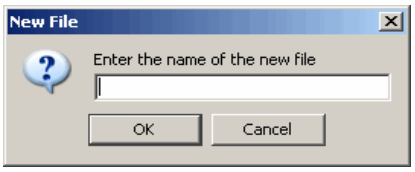
Table 21-3 File Manager Panel-Action buttons

Button Name	Description
New	Allows you to create a new text file and add it to the list of files.
Edit	Allows you to edit the file selected from a list of files.
Delete	Allows you to delete the selected file from the list of files.
Copy	Allows you to copy an existing file with a different name.
Rename	Allows you to rename the selected file from the list of files.
Refresh	Refreshes the file manager panel.

Creating a New File

Click the action button, **New**, to create a file in the 8950 AAA ***run*** directory. After the **New File** dialog appears, as shown in Figure 21-3, enter a unique file name and click **OK**.

Figure 21-3 New File Dialog



Enter the name of the file and click **OK**. The File Manager panel will display the name of the file that was entered with the list of files.

Open a File for Viewing or Editing

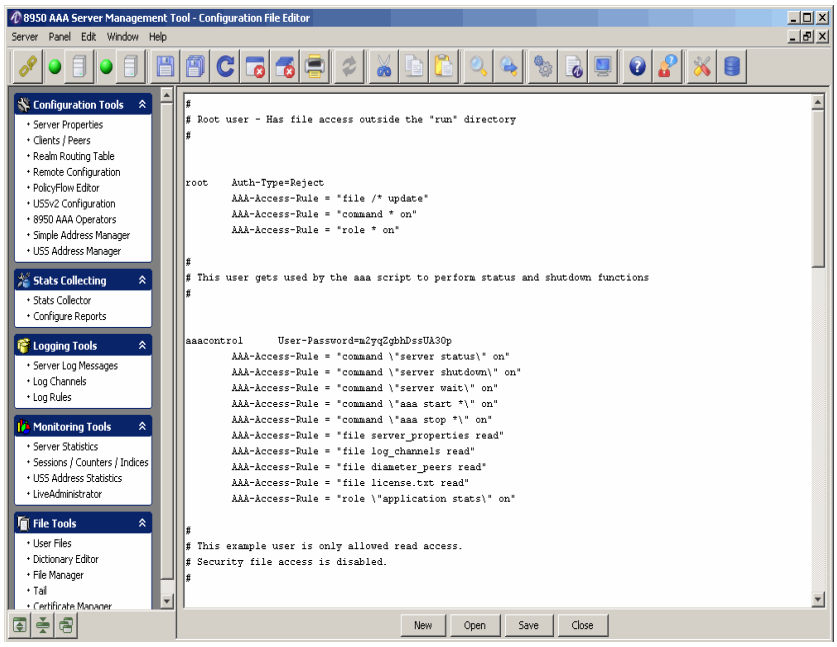
There are two ways to open a file for viewing or editing.

Double-click any entry in the list to open a Configuration File Editor panel showing the contents of the selected file. The file contents may be modified.

Click **Open As** to edit a file. A pop-up list appears with three editing selections, asking the user how to edit the selected file. The editing methods are:

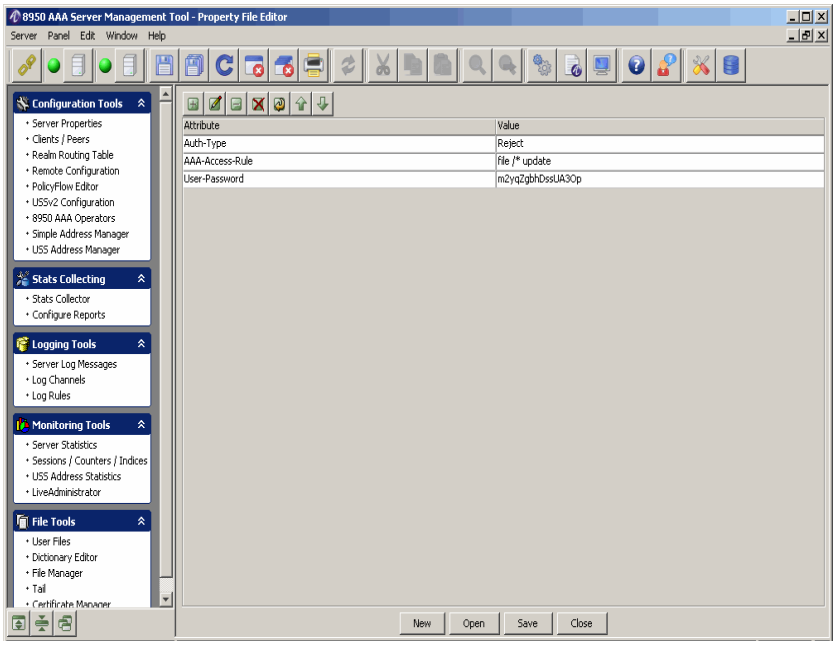
- **Plain text file** which opens the file in a Configuration File Editor panel. This option provides a simple text editing window similar to the Windows Notepad editor. An example is shown in Figure 21-4.

Figure 21-4 Editing a Plain Text File



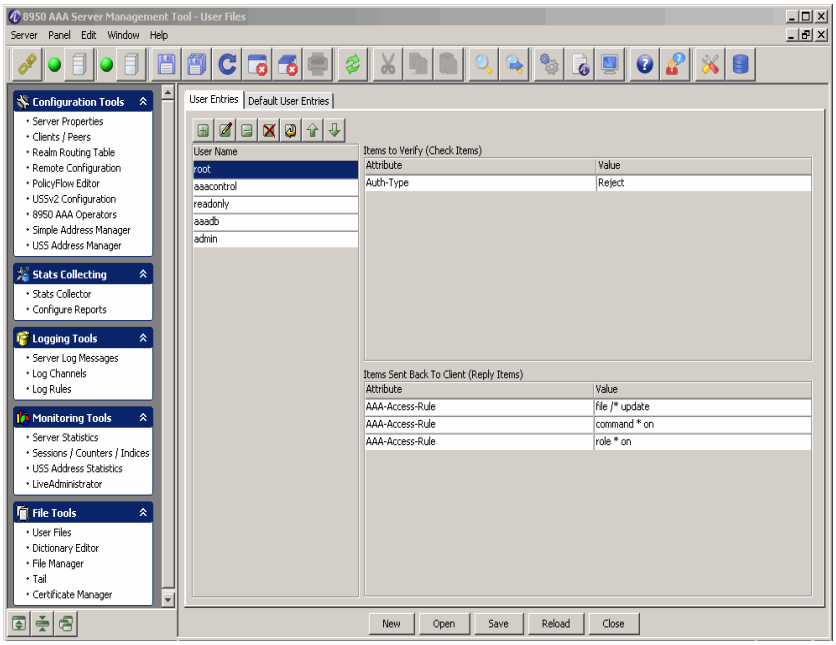
- **Property file** which opens the file in a Property File Editor panel.
  This GUI editor displays a set of properties and values. Selecting a value and clicking the edit button (or double clicking the property name) opens a separate editor window in which the property name and/or value can be changed. An example is shown in Figure 21-5.

Figure 21-5 Editing a Property File



- **User file** which opens the file in a User File panel. This editor option opens a file as a user file and uses the 8950 AAA SMT *User Files GUI* editor to edit the file. An example is shown in Figure 21-6.

Figure 21-6 Editing a User File



When finished editing the file, each panel provides the means to save the file and/or close the panel.

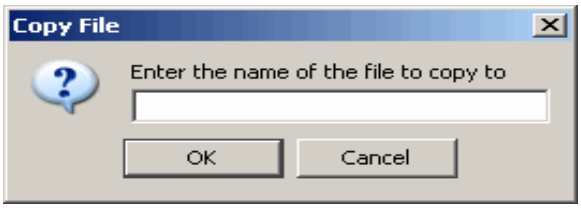
Copy a File

Click **Copy** to copy the contents of the selected file to a new file.

The Copy File dialog appears (Figure 21-7) requesting a name for the new file. To copy the file, enter the name and click **OK**.

The Copied file is saved in Run directory.

Figure 21-7 Copy File Dialog

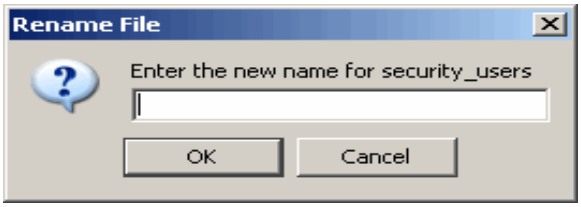


Rename a File

Select a file you want to be renamed from the File Manager Panel, Figure 21-1, and click **Rename** to name or change the name of an existing file.

The Rename File dialog appears (Figure 21-8) requesting the new name of the file. To rename the file, enter the name and click **OK**.

Figure 21-8 Rename File Dialog

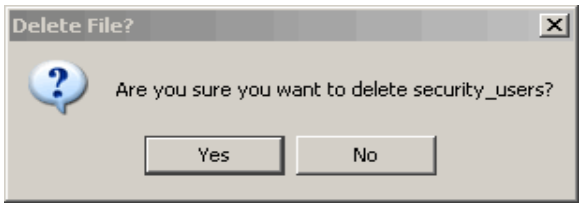


Delete a File

Select a file you want to be deleted from the File Manager Panel, Figure 21-1, and click Delete to remove the selected file from the list of files.

The Delete File dialog appears (Figure 21-9) requesting confirmation. To delete the file, click **Yes** else click **No**.

Figure 21-9 Delete File Dialog



Click Refresh File List action button to refresh the list after performing any of the operations discussed above.

Close

The **Close** button removes the File Manager panel from the SMT interface.

Tail panel

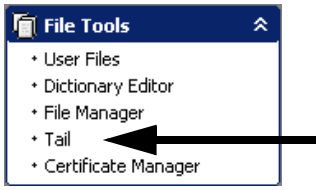
About Tail

The Tail panel enables the user to use or perform the Tail action, similar to the UNIX tail option, on the 8950 AAA files.

When you perform the tail option on a selected file, the standard output is put in this selected file at the designated place or at the end of the file. This is useful when monitoring the text that is being written to a file by another process.

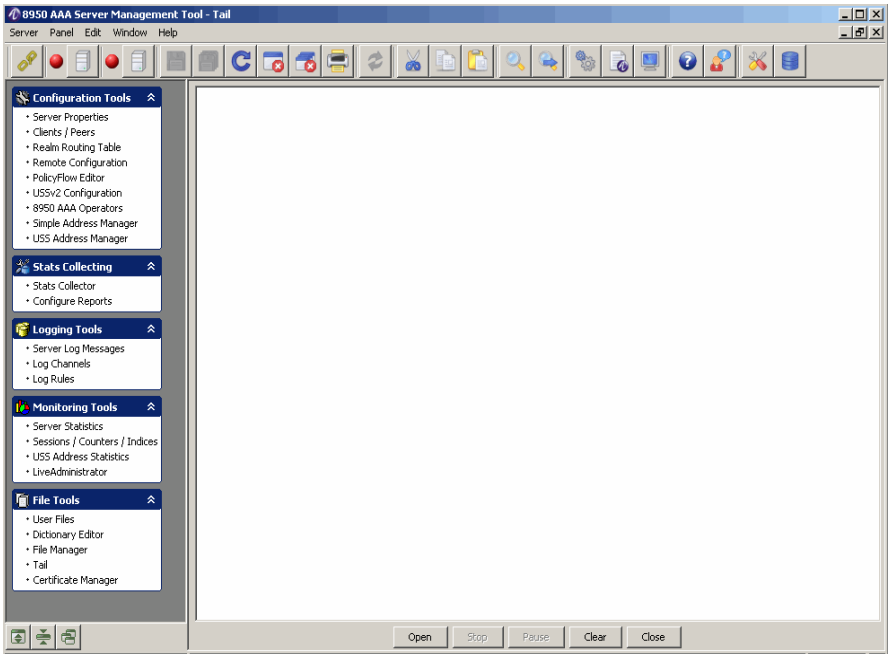
1. To display the Tail panel, select **Tail** from the Navigation Pane, under **File Tools**, as shown in Figure 21-10.

Figure 21-10 Navigation Pane-Tail



Result: The Tail panel is displayed, as shown in Figure 21-11.

Figure 21-11 Tail Panel

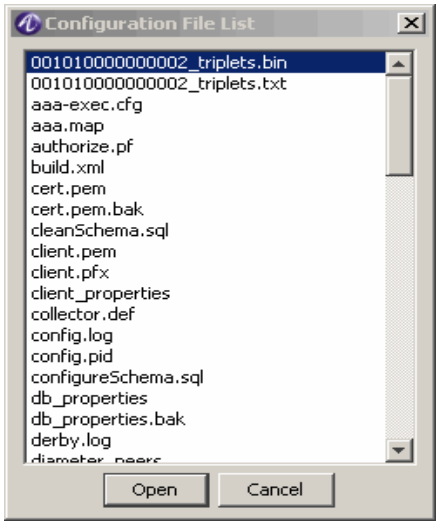


The Tail panel allows you to open an existing file from the list of 8950 AAA files.

2. To open existing file(s), click **Open**.

   Result: The Configuration File List dialog is displayed, as shown in Figure 21-12.

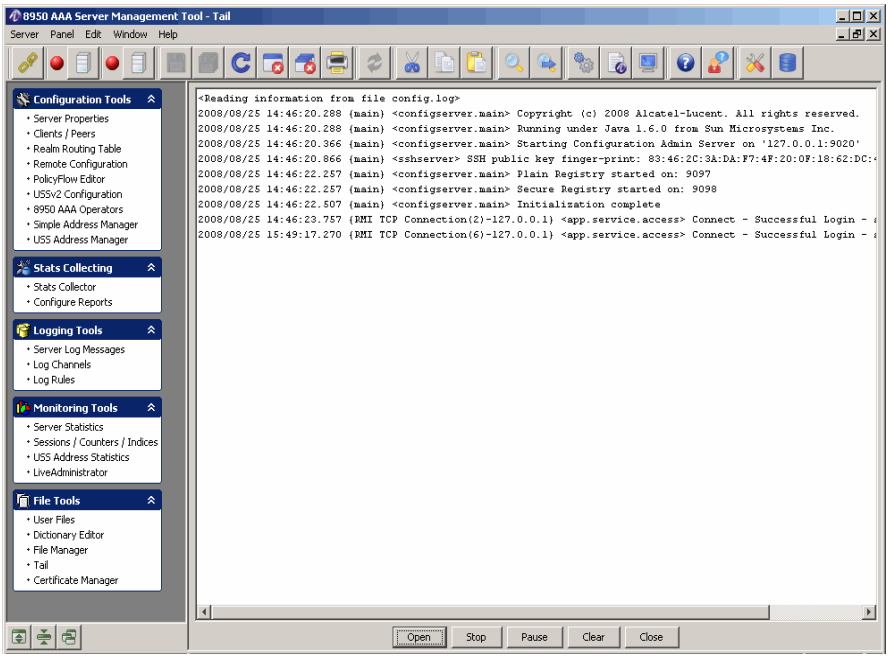
Figure 21-12 Configuration File List



3. Select the required file and click **Open**.

   Result: The Tail panel–with opened file is displayed, as shown in Figure 21-13.

Figure 21-13 Tail Panel-with opened file



4. You can Start or Stop, Pause, Clear, or Close the tail. Select the desired option.
5. Select **Close** to close the tail.

END OF STEPS

22 8950 AAA Certificate Manager

Overview

Purpose

This chapter discusses the 8950 AAA Certificate Manager, also known as *aaa-cert*. Root certificates generated with aaa-cert are *self-signed* certificates. This means that in order for a client or server to verify the certificates signed by an aaa-cert root certificate, they must install the root certificates as a trusted certificate authorities.

The following topics are included in this chapter:

Types of Certificates

About Types of certificates

The aaa-cert tool generates three types of certificates:

- Root Certificates
- Server Certificates
- Client Certificates

Root certificates are used to sign client and server certificates. For each root certificate it generates, aaa-cert creates a private and a public key. The private key is used to sign other certificates. The public key is used to verify other (server & client) certificates signed by the root certificate.

Server certificates are used by 8950 AAA to authenticate itself to remote clients. Server certificates are signed by a root certificate. In order to sign the server certificate, aaa-cert needs access to a root certificate and the private key associated with the certificate.

The aaa-cert tool can also be used to generate PKCS #10 Certificate Requests for a server certificate. This request can then be submitted to a certificate authority which will generate the server certificate. That functionality is not covered in this document.

Client certificates are used by clients to authenticate themselves to 8950 AAA. Client certificates are signed by a root certificate. In order to sign the server certificate, aaa-cert needs access to a root certificate and the private key associated with the certificate.

Important! For more information about Root, Server, and Client certificates, please refer to "Notes on Using Certificates" on page 20.

The Certificate Manager Panel

File manager panel

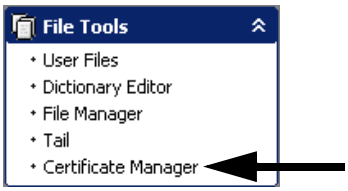
The Certificate Manager panel displays a list of certificates in the **run** directory of the PolicyServer. This panel enables the user to perform a variety of operations on the 8950 AAA Certificate Manager files. These operations include:

- Create Certificate
- View Certificate
- Delete a Certificate
- Copy the contents of a certificate to a new certificate
- Rename an existing certificate
- Refresh the list of certificates
- Copy the contents of a certificate to the clipboard

Important! All certificate operations are limited to the 8950 AAA run directory.

To display the Certificate Manager panel, select **Certificate Manager** from the Navigation Pane, under **File Tools**, as shown in Figure 22-1.

Figure 22-1 Navigation Pane-Certificate Manager

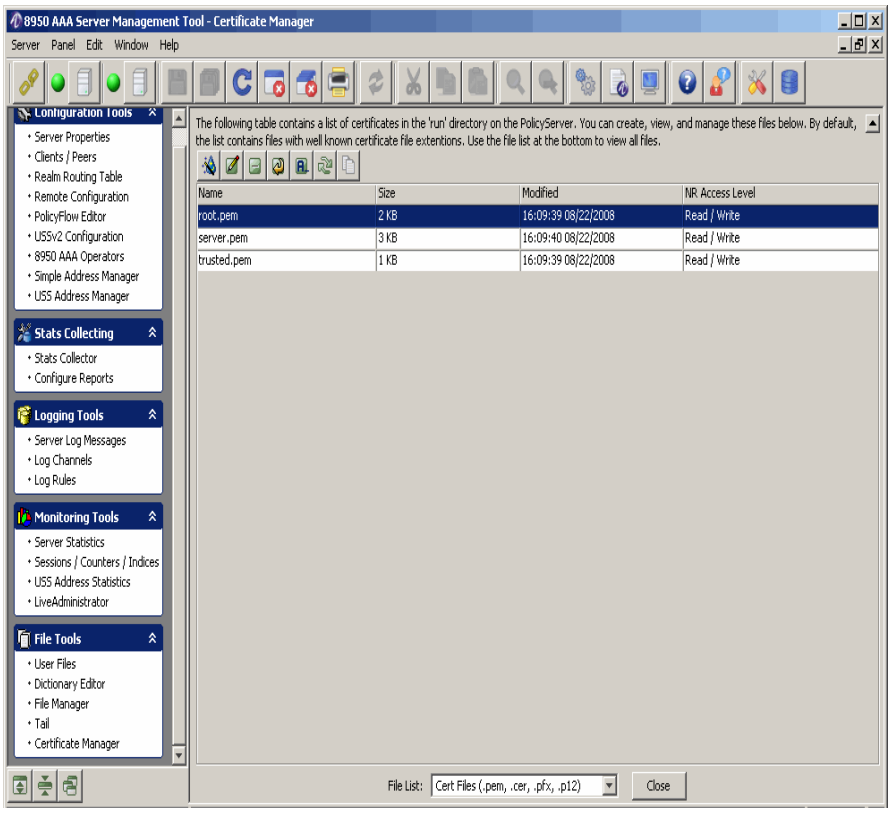


Viewing File Attributes and File Content

As shown in Figure 22-2, the Certificate File Manager panel displays the following attributes of a file:

- File Name
- File Size
- Date last modified
- NR Access Level

Figure 22-2 File Manager Panel



There are different types of files that are used by 8950 AAA Certificate Manager.

There are seven action buttons at the top of the Certificate Manager panel, as shown in Figure 22-3.

Figure 22-3 Certificate Manager panel-Action buttons

These are described in Table 22-1.

Table 22-1 Certificate Manager Panel-Action buttons

Button Name	Description
Create certificate	Allows you to create a new certificate file and add it to the list of files.
View certificate	Allows you to view and edit a certificate file from the list of files.
Delete	Allows you to delete the selected file from the list of files.
Copy	Allows you to copy an existing file as a different file with a different name.
Rename	Allows you to rename the selected file from the list of files.
Refresh	Refreshes the file manager panel.
Copy to clipboard	Allows you to copy the contents of the existing file into clipboard.

More information on Types of Certificates and how to create each types of certificates are explained in “Types of Certificates in Certificate Manager” on page 9.

Open a File for Viewing or Editing

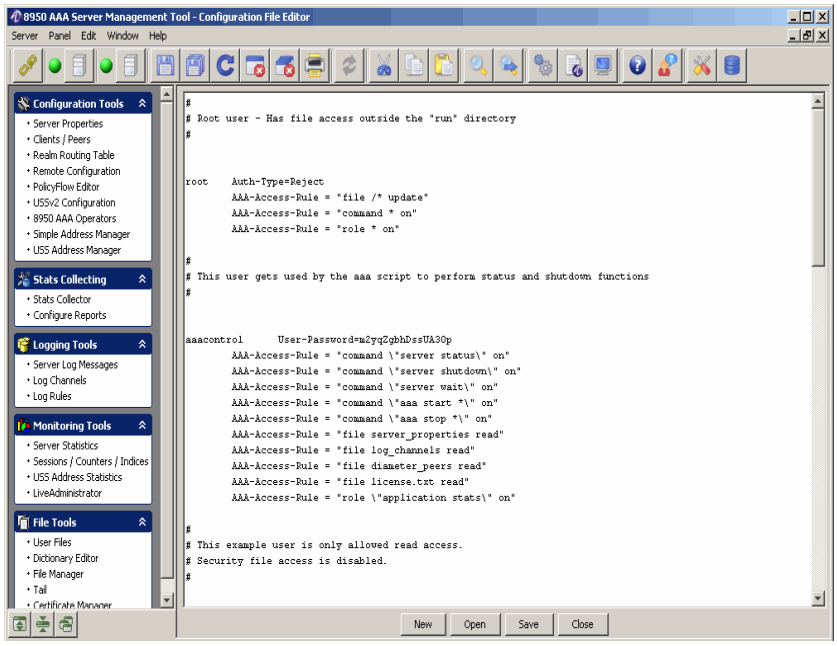
There are two ways to open a file for viewing or editing.

Double-click any entry in the list to open a Configuration File Editor panel showing the contents of the selected file. The file contents may be modified.

Click **Open As** to edit a file. A pop-up list appears with three editing selections, asking the user how to edit the selected file. The editing methods are:

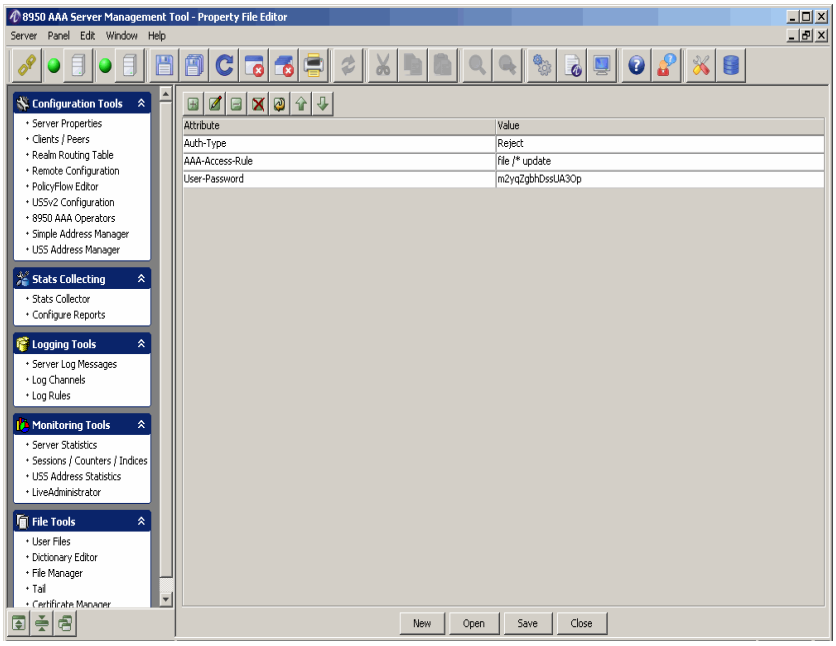
- **Plain text file** which opens the file in a Configuration File Editor panel.
  This option provides a simple text editing window similar to the Windows Notepad editor. An example is shown in Figure 22-4.

Figure 22-4 Editing a Plain Text File



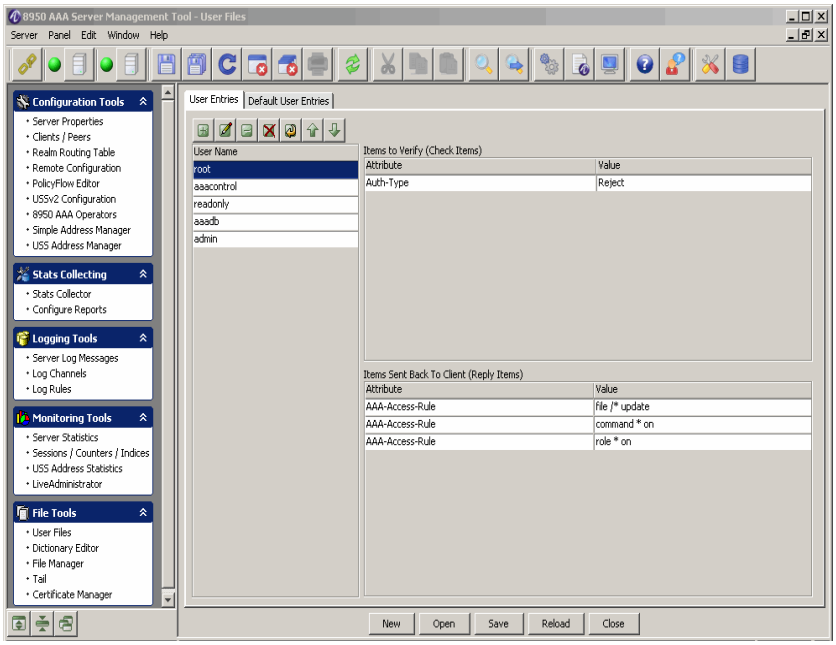
- **Property file** which opens the file in a Property File Editor panel.
  This GUI editor displays a set of properties and values. Selecting a value and clicking the edit button (or double clicking the property name) opens a separate editor window in which the property name and/or value can be changed. An example is shown in Figure 22-5.

Figure 22-5 Editing a Property File



- **User file** which opens the file in a User File panel.
  This editor option opens a file as a user file and uses the 8950 AAA SMT *User Files GUI* editor to edit the file. An example is shown in Figure 22-6.

Figure 22-6 Editing a User File



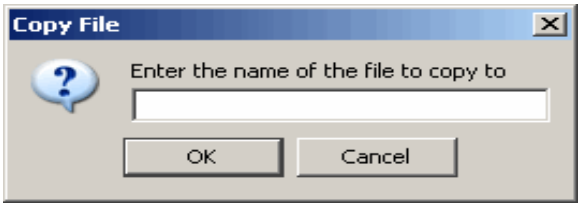
When finished editing the file, each panel provides the means to save the file and/or close the panel.

Copy a File

Click **Copy** to copy the contents of the selected file to a new file.

The Copy File dialog appears (Figure 22-7) requesting a name for the new file. To copy the file, enter the name and click **OK**.

Figure 22-7 Copy File Dialog

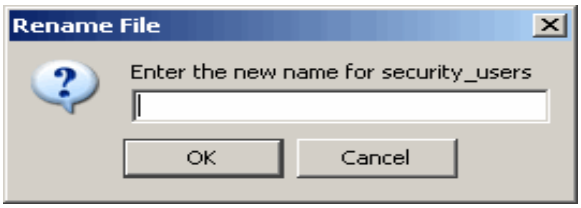


Rename a File

Select a file you want to be renamed from the File Manager Panel, Figure 22-2, and click **Rename** to name or change the name of an existing file.

The Rename File dialog appears (Figure 22-8) requesting the new name of the file. To rename the file, enter the name and click **OK**.

Figure 22-8 Rename File Dialog

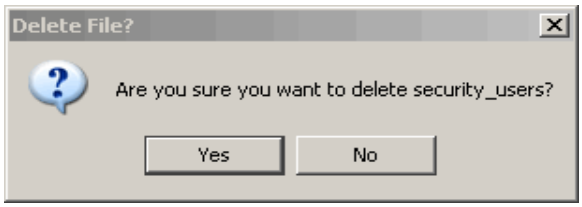


Delete a File

Select a file you want to be deleted from the File Manager Panel, Figure 22-2, and click Delete to remove the selected file from the list of files.

The Delete File dialog appears (Figure 22-9) requesting confirmation. To delete the file, click **Yes** else click **No**.

Figure 22-9 Delete File Dialog



Close

The **Close** button removes the File Manager panel from the SMT interface.

Requirements for Using the Certificate Manager

Requirements for the Certificate Manager

You must obtain or create a root certificate before you can create server or client certificates. You only need to create one root certificate for your site.

If your application uses protocols such as EAP-TTLS, EAP-PEAP etc. you will need a Root certificate and a Server certificate. Follow steps 1 and 2 below.

If you will be using EAP-TLS, you will need Root certificate, a Server certificate and one or more Client certificates. Follow the procedures defined in the next section, “Procedures for Creating Certificates”.

Important! The ncert utility saves all certificate files in the 8950 AAA run directory.

Types of Certificates in Certificate Manager

About the Types of Certificates

The Certificate Manager allows you to create different types of certificates and perform the options as described in Table 22-2.

Table 22-2 Certificate Manager–Types of Certificates

Certificate Types	Description
Root Certificate	Generates a key pair and a self signed root certificate which can be used to sign server and client certificates. This option creates a file containing the root certificate and encrypted private key and a trusted file for import into entities needing to validate certificates signed by this root.
Server Certificate	Generates a key pair and a server certificate which can be used to identify a server. The server certificate must be signed by a root certificate and the password for the root encrypted private key must be known. Typically the certificate and the private key generated by the root certificate selection above are used. The server certificate contains extensions suitable for server authentication.
Client Certificate	Generates a key pair and a client certificate which can be used to identify a client. The client certificate must be signed by a root certificate and the password for the root encrypted private key must be known. Typically the certificate and the private key generated by the root certificate selection above are used. The client certificate contains extensions suitable for client authentication.

Some additional properties of the Certificate type (also shown in Figure 22-10) are explained in Table 22-2

Table 22-3 Certificate Manager–Types of Certificate (Additional Properties)

Certificate Types	Description
Certificate Request	Generates a key pair and a PKCS # 10 certificate request which can be used to request a server certificate. The certificate request must be submitted to a certificate authority to generate a server certificate. The certificate authority will use its root certificate to sign the server certificate. The certificate request contains extensions suitable for server authentication.
View Existing Certificate	Views the contents of an existing certificate file. This includes PKCS #12 formatted certificates.

Creating New Certificates

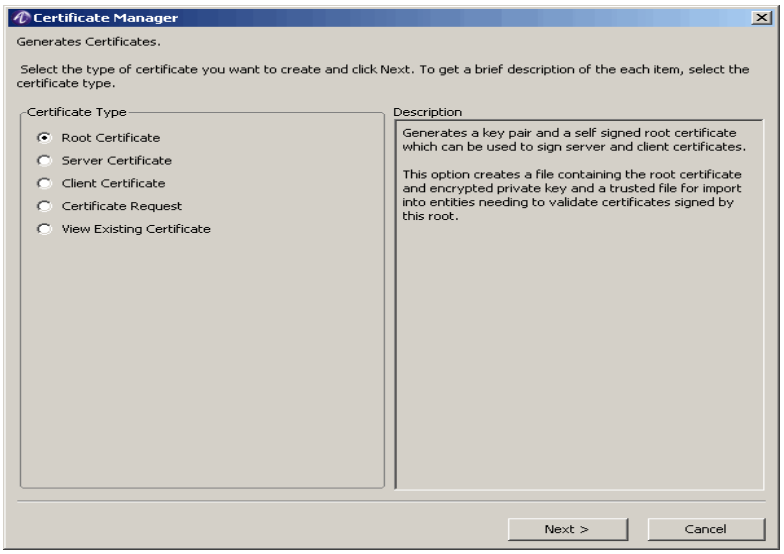
Each type of certificates, as specified in Table 22-3, have different parameters or properties to be filled in while creating a new certificate. These are explained in detail in the following sections.

Creating a New File for the Root Certificate type

1. Click the Create Certificate action button,  , to create a Certificate file in the 8950 AAA ***run*** directory.

   Result: The New Certificate dialog appears, as shown in Figure 22-10.

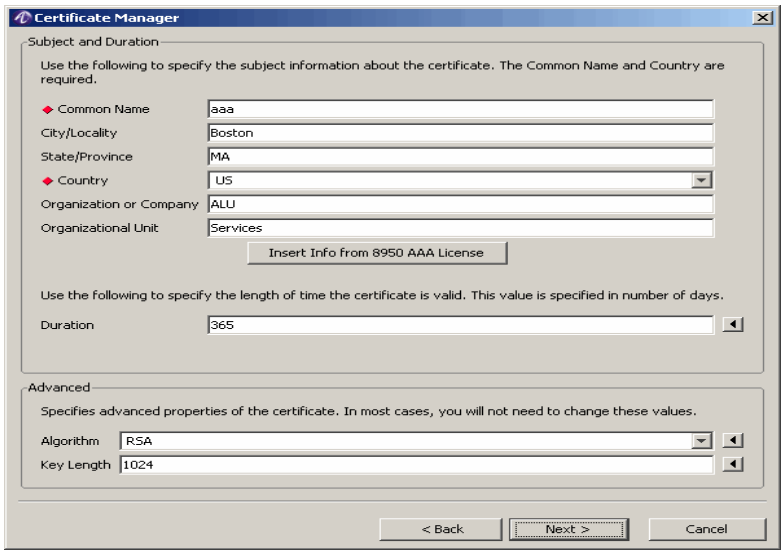
Figure 22-10 New Certificate Dialog-Certificate Type



2. Select the Certificate Type as **Root** and click **Next**.

   Result: The Root Certificate Type–Subject and Duration dialog is displayed, as shown in Figure 22-11.

Figure 22-11 Root Certificate Type-Subject and Duration

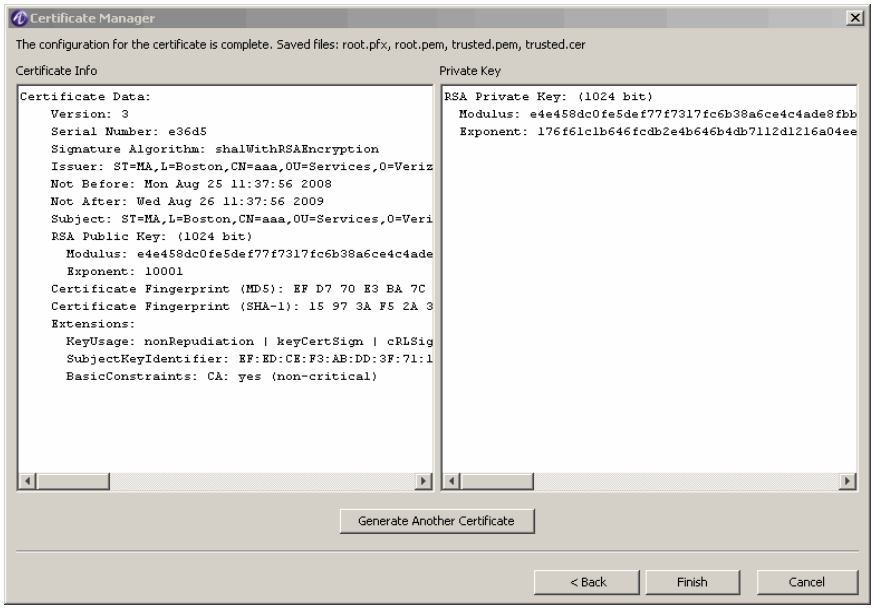


3. Use this screen to specify the subject information about the certificate. The fields, Common Name and the Country, are mandatory fields. Also specify the length of time the certificate is valid and specify the advanced properties of the certificate. Click **Next**.
4. The File Overwrite message box is displayed. This displays the list of files that already exist and asks if you want to overwrite them. Click **Yes** if you want to overwrite them and continue. Click **No** if you do not want to overwrite and return back.

Important! The file is overwritten only if it exist before. Otherwise, a new certificate is created.

Result: The Root Certificate Type–Certificate Complete dialog is displayed, as shown in Figure 22-12.

Figure 22-12 Root Certificate Type-Certificate Complete



5. Click **Finish** to go back to the File Manager panel as shown in Figure 22-2.

Creating a New File for the Server and Client Certificate types

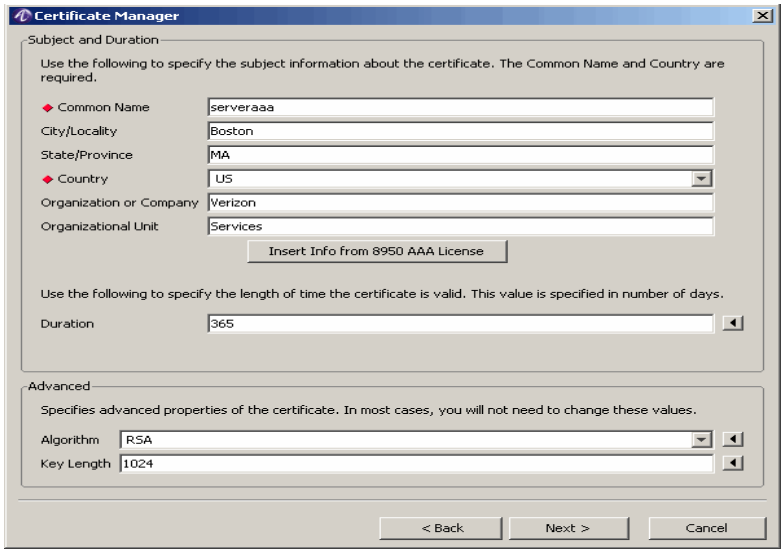
1. Click the Create Certificate action button,  .

   Result: The New Certificate dialog appears, as shown in Figure 22-10.

2. Select the Certificate Type as either **Server** or as **Client** and click **Next**.

   Result: The Server or Client Certificate Type–Subject and Duration dialog is displayed, as shown in Figure 22-13.

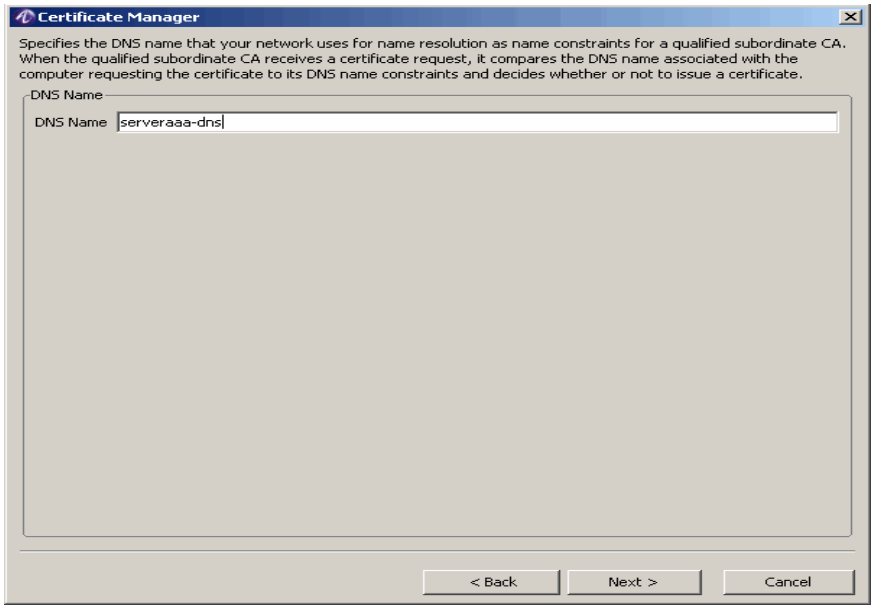
Figure 22-13 Server/Client Certificate Type-Subject and Duration



3. Use this screen to specify the subject information about the certificate. The fields, Common Name and the Country, are mandatory fields. Also specify the length of time the certificate is valid and specify the advanced properties of the certificate. Click **Next**.

   Result: The Server or Client Certificate Type–DNS Name dialog is displayed, as shown in Figure 22-14.

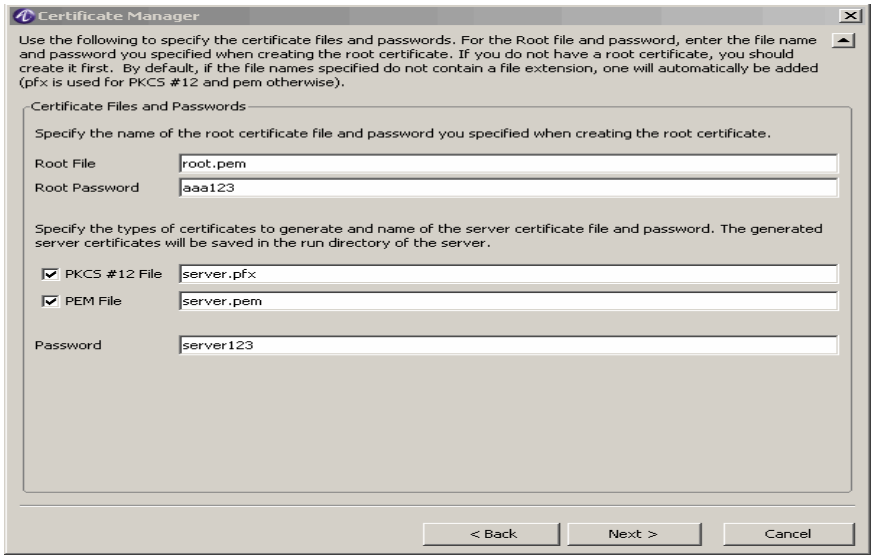
Figure 22-14 Server/Client Certificate Type-DNS Name dialog



4. Specify the DNS name that your network uses for name resolution. Enter the DNS name and click **Next**.

Result: The Server or Client Certificate Type–Certificate Files and Passwords dialog is displayed, as shown in Figure 22-15.

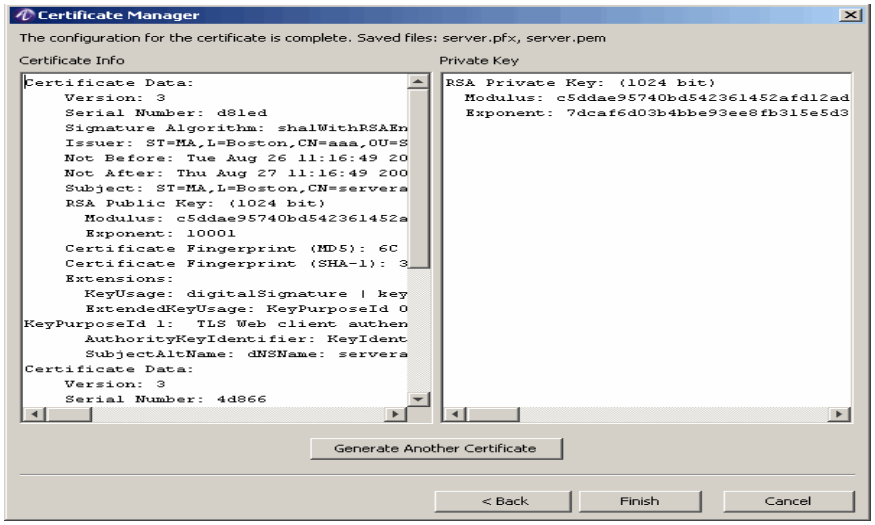
Figure 22-15 Server/Client Certificate Type–Certificate Files and Passwords dialog



5. Specify the certificate files and passwords. For the Root file and password, enter the file name and password you specified when creating the root certificate. Click **Next**.

Result: The Server or Client Certificate Type–Certificate Complete dialog is displayed, as shown in Figure 22-16.

Figure 22-16 Server/Client Certificate Type-Certificate Complete



Important! The process to get Server or Client Certificates is same. You need to specify which certificate you need and specify the parameters accordingly to get the Server or Client certificate.

6. Click **Finish** to go back to the File Manager panel as shown in Figure 22-2.

Requesting for a Certificate

This dialog or panel generates a key pair and a PKCS #10 certificate request which can be used to request a server certificate.

The certificate request must be submitted to a certificate authority to generate a server certificate. The certificate authority will use its root certificate to sign the server certificate. The certificate request contains extensions suitable for server authentication.

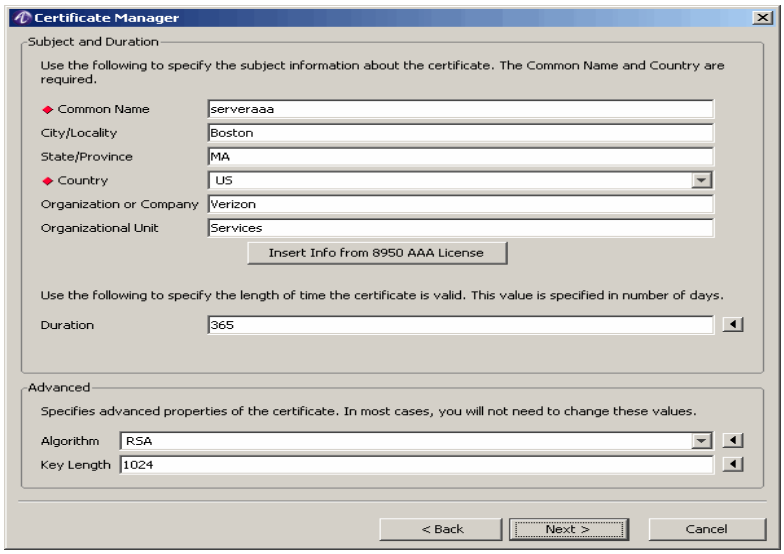
1. Click the Create Certificate action button,  .

   Result: The New Certificate dialog appears, as shown in Figure 22-10.

2. Select the Certificate Type as **Certificate Request** and click **Next**.

   Result: The Server or Client Certificate Type–Subject and Duration dialog is displayed, as shown in Figure 22-17.

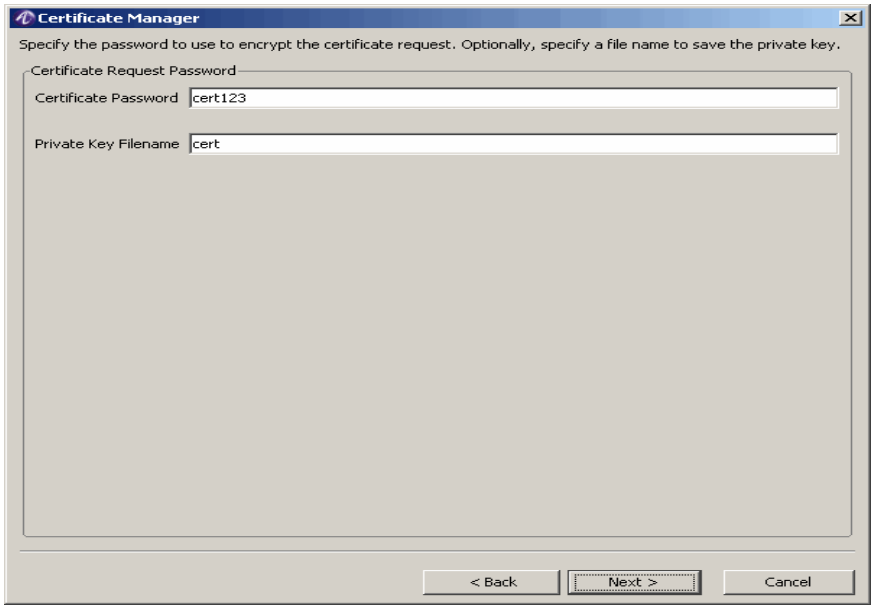
Figure 22-17 Certificate Request-Subject and Duration



3. Check if the information is correct and as you entered about the certificate. If required, modify and click **Next**.

   Result: The Certificate Request Password dialog is displayed, as shown in Figure 22-18.

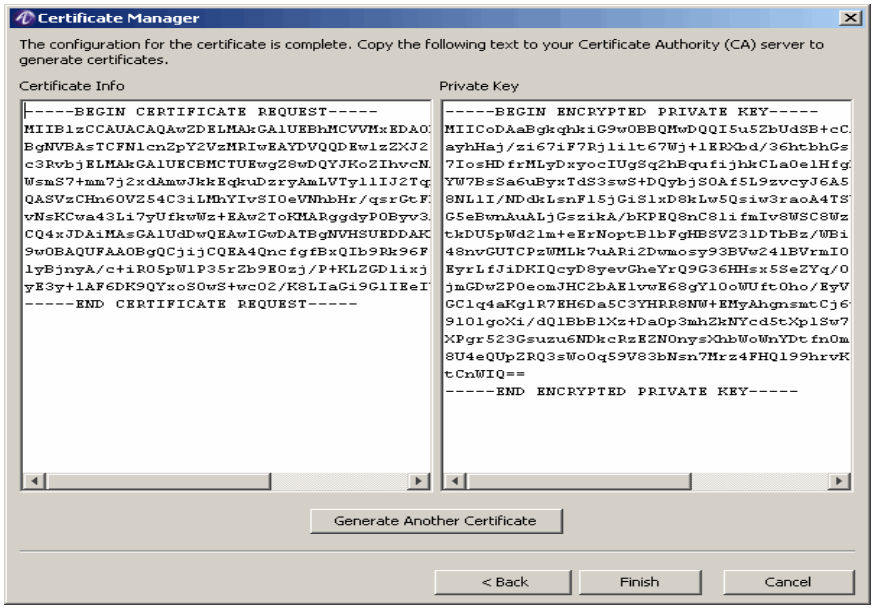
Figure 22-18 Certificate Request Password dialog



4. Specify the password to use to encrypt the certificate request. Optionally, specify a file name to save the private key. Click **Next**.

   Result: The Certificate Request Complete dialog is displayed, as shown in Figure 22-19.

Figure 22-19 Certificate Request Complete



5. Click **Finish** to go back to the File Manager panel as shown in Figure 22-2.

Viewing an existing Certificate

This dialog or panel allows you to select the type of certificate you want to create.

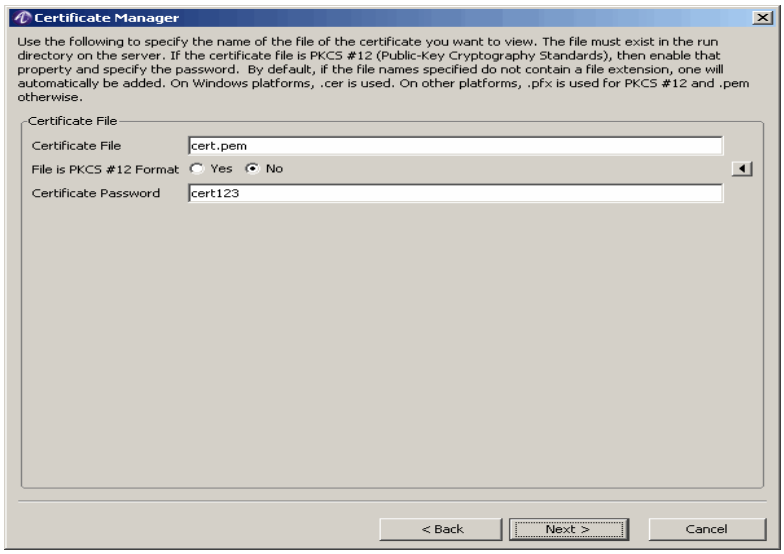
1. Click the Create Certificate action button,  .

   Result: The New Certificate dialog appears, as shown in Figure 22-10.

2. Select the **View Existing Certificate** and click **Next**.

   Result: The View Existing Certificate–Certificate File is displayed, as shown in Figure 22-20.

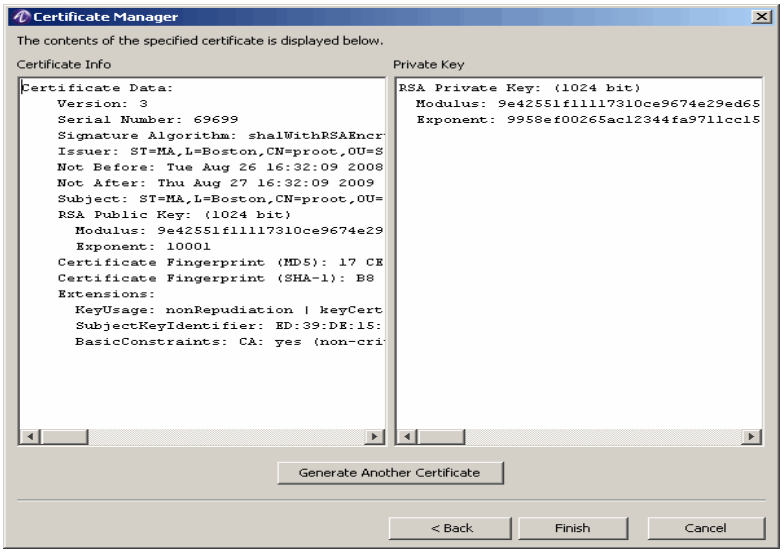
Figure 22-20 View Existing Certificate-Certificate File



3. Specify the name of the file of the certificate that you want to view. The file must exist in the run directory on the server. If the certificate file is PKCS #12 (Public-key Cryptography Standards), then enable that property and specify the password. By default, if the file names specified do not contain a file extension, one will automatically be added. On Windows platforms, .cer is used. On other platforms, .pfx is used for PKCS #12 and .pem otherwise. Click **Next**.

   Result: The Certificate Information dialog is displayed, as shown in Figure 22-21.

Figure 22-21 Certificate Information



4. Click **Finish** to go back to the File Manager panel as shown in Figure 22-2.

Procedures for Creating Certificates

Generating a Root Certificate

Important! Do not run this procedure if you already have a self-signed root certificate.

1. From the 8950 AAA **bin** directory enter the following: `./aaa-cert -gui`
2. From the GUI select **Root Certificate** and click **Next** >
3. Enter a **Common Name** for your Root certificate, for example, MyRootCert.
4. Enter your country if it is other than the US.
5. Add any additional information and click **Next** >
6. Enter the password for encrypting the root certificate private key and click **Next** >
7. Enter the names of the certificate and trusted files, or accept the defaults, and click **Next** >
8. **Result**: The contents of the certificate are displayed for your review. It is not necessary to record this information; it will be included in the file.
9. Click **Generate Another Certificate** to create a server certificate or a client certificate

   OR

   click **Close** to terminate the aaa-cert application.

Generating a Server Certificate

Important! You must have a server certificate for certain EAP types, for example: EAP-TLS, EAP-TTLS, EAP-PEAP.

1. If the aaa-cert GUI is not open, from the 8950 AAA **bin** directory, type:

   ```
   ./aaa-cert -gui
   ```

2. From the GUI select **Server Certificate** and click **Next** >
3. Enter a **Common Name** for your server certificate, for example, MyServerCert.
4. Enter your country if it is other than the US.
5. Enter the number of days to specify the validity of the certificate.
6. Add any additional information and click **Next** >
7. Enter the GNS name and click **Next** >
8. Enter the root file name and the password used to encrypt the root certificate private key.
9. Enter the password for encrypting the server certificate private key.

   Important! Record the password in a safe place. You will need it to generate server and client certificates.

10. Click **Next** >
11. Enter the name of the root certificate file. See “Generating a Root Certificate” on page 18.
12. Enter a name for the server certificate file you are creating, or accept the defaults, and click **Next** >
13. The contents of the certificate are displayed for your review. It is not necessary to record this information; it will be included in the file.
14. Click **Generate Another Certificate** to create a client certificate

    OR

    click **Close** to terminate the aaa-cert application.

Generating a Client Certificate

Important! You must have a client certificate for certain EAP types, for example: EAP-TLS, EAP-TTLS, EAP-PEAP.

1. If the aaa-cert GUI is not open, from the 8950 AAA **bin** directory type:

   ```
   ./aaa-cert -gui
   ```

2. From the GUI select **Client Certificate** and click **Next** >
3. Enter a **Common Name** for your client certificate, for example, MyClientCert.
4. Enter your country if it is other than the US.

5. Add any additional information and click **Next** >
6. Enter the password used to encrypt the root certificate private key.
7. Enter the password for encrypting the client certificate private key and click **Next** >
8. Enter the name of the root certificate file. See “Generating a Root Certificate” on page 18.
9. Enter a name for the client certificate file you are creating, or accept the defaults.

   Important! If you are creating multiple client certificates, be sure to save each one is a separate file.
10. Click **Next**.

    Result: The contents of the certificate are displayed for your review. It is not necessary to record this information; it will be included in the file.
11. Click **Generate Another Certificate** to create another Client certificate

    OR

    click **Close** to terminate the aaa-cert application.

Notes on Using Certificates

Root Certificates

Root certificate files generated by aaa-cert contain an encoded X.509 certificate with extensions for a certificate authority and the encrypted private key matching the public key in the root certificate. A password is used to encrypt the private key and protect it from public access.

Root certificates are signed with their own private key and therefore cannot be verified by another certificate. Typically root certificates are verified by checking a digital fingerprint published in a secure manner. Root certificates are installed on machines that need to verify client and server certificates signed by the root certificate.

Rather than using aaa-cert to generate a root certificate, a root certificate from another source, including another installation of 8950 AAA could be used for your site. However, when using aaa-cert you must always have the private key for the Root certificate you will be using and know the password used to encrypt the private key.

Server and Client Certificates

Server and Client certificate files generated by aaa-cert for contain: an encoded X.509 certificate with extensions for server or client authentication; the X.509 certificate used to sign the certificate; and the encrypted private key matching the public key in the certificate. A password is used to encrypt the private key and protect it from public access.

How to Configure for a TLS Demo Out of the Box

Configuring the TLS Demo

Important! The following is a sample session showing the procedure to run TLS. It starts from a new install using the PolicyAssistant. This sample session also shows how to test using the command line version of nrtest.

```
c:\work\nr43\release\build>prompt=-$G
->setup.bat -dir
C:\work\8950AAA -agree -server -adminUser admin -
adminPass admin -nogui
-------------------------------------------------------------
8950AAA Setup, Version 5 Copyright (c) 2008 Alcatel-Lucent. All
   Rights Reserved.
You are about to install 8950AAA.
Enter 'X' at any prompt to exit the setup program.

Using Java version:
Java(TM) 2 Runtime Environment, Standard Edition
Sun Microsystems Inc.
Version: 1.5.0
From: 'C:\Program Files\Java\j2re1.5.0'

8950AAA.
PolicyAssistant is a predefined PolicyFlow that retrieves user
   information from an LDAP Directory, RADIUS User File,
   Database,or Remote RADIUS Server. User authentication can be
   done byWindows NT, Unix, Plain Text Passwords, SecurID and
   SafeWord.
Note: Don't install the PolicyAssistant if you want to create your
   own PolicyFlow.
Do you want to install the PolicyAssistant : Y
Setting up for reading entries
Installing files to C:\work\8950AAA
.............................................................
   .............................................................
   .............................................................
   .............................................................
   ................
Copying File - accounting.old.sql
Copying File - acct.hsqldbCopying File - acct_methods
Copying File - auth.hsqldb
Copying File - authentication.old.sql
Copying File - auth_methods
Copying File - clean.hsqldb
Copying File - data.config-info
```

```
Copying File - data.dnis-info.csv
Copying File - data.realm-info.csv
Copying File - initial.hsqldb
Copying File - Jdbc.acct_insert.map
Copying File - Jdbc.acct_insert.sql
Copying File - Jdbc.acct_insert_active.sql
Copying File - Jdbc.acct_move.sql
Copying File - Jdbc.acct_update.map
Copying File - Jdbc.acct_update.sql
Copying File - Jdbc.old.acct_insert.map
Copying File - Jdbc.old.acct_insert.sql
Copying File - Jdbc.old.acct_update.map
Copying File - Jdbc.old.acct_update.sql
Copying File - log.hsqldb
Copying File - method_select
Copying File - policyassistant_properties
Copying File - readme.txt
Copying File - users
Copying File - users.templates
Copying File - uss_counters
Updating Server Properties
Updating Security Properties
Updating SMT Properties
Setting Up Database
Copying License File
Copying File - nr.jar
Copying File - xerces.jar
Copying File - jakarta-oro.jar
Setting up for uninstall
Installation Completed Successfully
->cd \work\8950AAA\run\
->pwd
C:/work/8950AAA/run
->..\bin\aaa-cert -gui
Selected "Root Certificate" and filled out as in attachments
   root1.jpg to root4.jpg
Selected "Generate Another"
Selected "Server Certificate" and filled out as in attachments
   server1.jpg to server4.jpg
Selected "Generate Another"
Selected "Client Certificate" and filled out as in attachments
   client1.jpg to client4.jpg
Exited App
->ls -l *pem
-rwxrwxrwa   1 Administrators None              2918 Mar 1 22:42
   client.pem-rwxrwxrwa   1 Administrators None              1954
```

```
   Mar 1 22:42 root.pem-rwxrwxrwa  1 Administrators None
   2918 Mar 1 22:42 server.pem-rwxrwxrwa  1 Administrators None
   944 Mar 1 22:35 trusted.pem
Started SMT....
->..\bin\nrsmt -u admin -p admin -l
Configured PolicyAssistant accepting all of the included samples
   defaults up until the Authentication Page.
Expanded EAP section in Authentication types
Selected EAP-TLS, clicked next
Accepted defaults until TLS page. Used info in tls1.jpg.
Accepted defaults for rest and selected save
exited SMT.
Now have policy of:
->cat data.config-info
MyPolicy
PolicyName="MyPolicy"
User-Source="UserFile"
Default-AuthType="EAP-TLS"
Asserted-Auth-Type="FALSE"
Connection-Limit="1"
Policy-Limit="-1"
User-Limit-Scope="Policy"
UserFileName="users"
 Proxy-Acct-Enabled="FALSE"
User-Template-Enabled="FALSE"
Session-Templates-Enabled="TRUE"
Policy-Templates-Enabled="TRUE"
Template-FileName="users.templates"
Policy-Session-Template="PPP"
Disposition-On-Missing-Template="success"
EAP-Allowed-Auth-Types="EAP-TLS"
TLS-RsaCertFile="server.pem"
TLS-RsaKeyPassword="test-server"
TLS-TrustedFile="trusted.pem"
TLS-FragmentSize="1012"
Allowed-Transports="/EAP-TLS/EAP-TLS"
Tunnel-Enabled="FALSE"
TTLS-RsaCertFile="server.pem"
TTLS-RsaKeyPassword="test-server"
Accounting-Method="DetailFile"
Accounting-FileName="detail"
Accounting-FileRolloverMode="Monthly"
->..\bin\va start radius -loglevel debug
8950AAA Radius Server starting...
8950AAA Radius Server initialized.
```

```
Create a small tuple file using notepad:
->cat tuple.txt
User-Name = steve
NAS-IP-Address = 127.0.0.1
NAS-Port = 1
And launch the RADIUS test tool in EAP-TLS mode to check:
->..\bin\nrtest -f tuple.txt -cbc EapTls$SimpleCallback -id steve
   -cfclient.pem -cp test-client -tf trusted.pem -v
Xmit: Access-Request
       User-Name = "steve"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
        EAP-Message = "Response/Identity(1): data=steve"
        Message-Authenticator = "00000000000000000000000000000000"

Packet authenticator is valid
Recv: Access-Challenge after 1953 ms.
        Message-Authenticator = "60B6D929DFE86EE6C1BA69C0F267EFD9"
        State = "1"
        Session-Timeout = 180
        EAP-Message = "Request/EAP-TLS(2): flags=20(S) "

Sending a 0 byte message to the EAP TLS client:
Received a 108 byte message from the EAP TLS client:
        Handshake,v3.1
          ClientHello
            version 3.1
            random =
404431C306BC65BFD2EDC94DF4D768528F6F1A0F86BAA9D00CF94E100187
6D70
            session_id =
            cipher_suites
              TLS_RSA_WITH_AES_256_CBC_SHA
              TLS_DHE_DSS_WITH_AES_256_CBC_SHA
              TLS_DHE_RSA_WITH_AES_256_CBC_SHA
              TLS_DH_DSS_WITH_AES_256_CBC_SHA
              TLS_DH_RSA_WITH_AES_256_CBC_SHA
              TLS_RSA_WITH_3DES_EDE_CBC_SHA
              TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
              TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
              TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
              TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
              TLS_RSA_WITH_AES_128_CBC_SHA
              TLS_DHE_DSS_WITH_AES_128_CBC_SHA
              TLS_DHE_RSA_WITH_AES_128_CBC_SHA
```

```
                    TLS_DH_DSS_WITH_AES_128_CBC_SHA
                    TLS_DH_RSA_WITH_AES_128_CBC_SHA
                    TLS_RSA_WITH_DES_CBC_SHA
                    TLS_DHE_DSS_WITH_DES_CBC_SHA
                    TLS_DHE_RSA_WITH_DES_CBC_SHA
                    TLS_DH_DSS_WITH_DES_CBC_SHA
                    TLS_DH_RSA_WITH_DES_CBC_SHA
                    TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
                    TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
                    TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
                    TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
                    TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
                    TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
                    TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
                    TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
                    TLS_DH_anon_WITH_AES_256_CBC_SHA
                    TLS_DH_anon_WITH_AES_128_CBC_SHA
                  compression_methods
                    NULL

Xmit: Access-Request
        User-Name = "steve"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
       Message-Authenticator = "00000000000000000000000000000000"
        EAP-Message = "Response/EAP-TLS(2): flags=80(L)
 msg.length=108frag.length=108"
        State = "1"

Packet authenticator is valid
Recv: Access-Challenge after 80 ms.
       Message-Authenticator = "C3A04508C76346818988A473A60DA9FF"
        State = "2"
        Session-Timeout = 180
        EAP-Message = "Request/EAP-TLS(3): flags=C0(LM)
  msg.length=1515
 frag.length=1002"

Acking TLS fragment
Xmit: Access-Request
        User-Name = "steve"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
       Message-Authenticator = "00000000000000000000000000000000"
        EAP-Message = "Response/EAP-TLS(3): flags=00()"
```

```
        State = "2"

Packet authenticator is valid
Recv: Access-Challenge after 30 ms.
       Message-Authenticator = "95224CCC2B120F28B9269A5A43BB17AE"
        State = "3"
        Session-Timeout = 180
        EAP-Message = "Request/EAP-TLS(4): flags=00()
  frag.length=513"
Sending a 1515 byte message to the EAP TLS client:
        Handshake,v3.1
          ServerHello
            version 3.1
            random =
 404431C5EC97CB06362A839E2844835F197242365A832C2F5D4B7060E46C55C
B
            session_id = 4617932DD7F525296FCADC70844DD701
            cipher_suite = TLS_RSA_WITH_3DES_EDE_CBC_SHA
            compression_method = NULL
          Certificate
          CertificateRequest
          ServerHelloDone

Received a 1646 byte message from the EAP TLS client:
        Handshake,v3.1
          Certificate
          ClientKeyExchange
        Handshake,v3.1
          CertificateVerify
        ChangeCipherSpec,v3.1
        Handshake,v3.1
          Finished

Xmit: Access-Request
        User-Name = "steve"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
       Message-Authenticator = "00000000000000000000000000000000"
        EAP-Message = "Response/EAP-TLS(4):
  flags=C0(LM)msg.length=1646
 frag.length=1002"
        State = "3"

Packet authenticator is valid
Recv: Access-Challenge after 10 ms.
```

```
        Message-Authenticator = "84752505CFB9AE3678B6013BDFDE3F32"
        State = "4"
        Session-Timeout = 180
        EAP-Message = "Request/EAP-TLS(5): flags=00() "

Xmit: Access-Request
        User-Name = "steve"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
        Message-Authenticator = "00000000000000000000000000000000"
        EAP-Message = "Response/EAP-TLS(5): flags=00()
  frag.length=644"
        State = "4"

Packet authenticator is valid
Recv: Access-Challenge after 331 ms.
        Message-Authenticator = "136C3CE06532EB5D3787339DADEB32DC"
        State = "5"
        Session-Timeout = 180
        EAP-Message = "Request/EAP-TLS(6): flags=80(L)
  msg.length=51frag.length=51"

Sending a 51 byte message to the EAP TLS client:
        ChangeCipherSpec,v3.1
        Handshake,v3.1
          Finished

Handshake Complete:
        Cipher suite = SSL_RSA_WITH_3DES_EDE_CBC_SHA
        Session ID =
  id:46:173:2D7:F5:25:29:6F:CAC0:84:4D7:01Acking TLS
 fragment
Xmit: Access-Request
        User-Name = "steve"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
        Message-Authenticator = "00000000000000000000000000000000"
        EAP-Message = "Response/EAP-TLS(6): flags=00()"
        State = "5"

Packet authenticator is valid
Recv: Access-Accept after 80 ms.
        Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-IP-Address = 192.168.10.6
```

```
        Framed-IP-Netmask = 255.255.255.255
        Framed-Routing = Broadcast-Listen
        Filter-Id = "std.ppp"
        Framed-MTU = 1500
        Framed-Compression = Van-Jacobson-TCP-IP
       Message-Authenticator = "A68A3FFF3FABCADFDCAB9E5DBE2F561B"
        MS-MPPE-Recv-Key =
 F4BF4E108DF391ED40FB9CD5F20734C45D503F3CAFDDBC72E242C7E90F8
83CC0
        MS-MPPE-Send-Key =
9613F55C951DB46E298647818E8771E04392FEA91E62337C6315332A36C484F
6
        EAP-Message = "Success(6)"
requests: 6
    access-request     : 6
        with State         : 5
        without State      : 1
    accounting-request : 0
    other-request      : 0
replies:  6
    access-accept      : 1
        with state         : 0
        without state      : 1
    access-reject      : 0
    access-challenge   : 5
        with state         : 5
        without state      : 0
    account-response   : 0
    other-response     : 0
timeouts: 0
errors:   0
retries:  0
miscErrs: 0
transaction count: 1
elapsed time(ms):  3065
trans per second:  0.3262642740619902
seconds per tran:  3.065

->tail -40 policy.log
  2864  <plugin.Compare.#AutoCheckLeftovers> Input2 = ''.
  2864  <plugin.Compare.#AutoCheckLeftovers> Operator is '=='.
 2864  <plugin.Compare.#AutoCheckLeftovers> SUCCESS -- Comparison
  is true.
  2864  <engine.worker.9> ACCEPT -- AutoChecks complete
  2864  <engine.worker.9> #AutoCheckLeftovers exits by ACCEPT --
```

```
  AutoChecks
 complete
  2864  <engine.worker.9> Reply encode:
        Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-IP-Address = 192.168.10.6
        Framed-IP-Netmask = 255.255.255.255
        Framed-Routing = Broadcast-Listen
        Filter-Id = "std.ppp"
        Framed-MTU = 1500
        Framed-Compression = Van-Jacobson-TCP-IP
        EAP-Message = "Success(6)"
       Message-Authenticator = "00000000000000000000000000000000"
        MS-MPPE-Recv-Key
 =F4BF4E108DF391ED40FB9CD5F20734C45D503F3CAFDDBC72E242C7E90
F883CC0
        MS-MPPE-Send-Key
 =9613F55C951DB46E298647818E8771E04392FEA91E62337C6315332A36C484
F6

  2874  <engine.worker.9> Reply attribute dump
        Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-IP-Address = 192.168.10.6
        Framed-IP-Netmask = 255.255.255.255
        Framed-Routing = Broadcast-Listen
        Filter-Id = "std.ppp"
        Framed-MTU = 1500
        Framed-Compression = Van-Jacobson-TCP-IP
        EAP-Message = "Success(6)"
       Message-Authenticator = "00000000000000000000000000000000"
        MS-MPPE-Recv-Key
 =F4BF4E108DF391ED40FB9CD5F20734C45D503F3CAFDDBC72E242C7E90
F883CC0
        MS-MPPE-Send-Key
 =9613F55C951DB46E298647818E8771E04392FEA91E62337C6315332A36C484
F6

2004/03/01 23:04:20.006 <stateserver.entry.timeout> State change:
waiting-for-start to inactive
        entry: 127.0.0.1+1 INACTIVE complete
          mod: Mon Mar 01 23:04:20 PST 2004
           ev: Mon Mar 01 23:03:34 PST 2004
          exp: <none>
```

END OF STEPS

Part VI: Database Tools Navigation Pane

Overview

Purpose

This part consolidates the chapter(s) related to Database Tools in the SMT Navigation pane.

Contents

This part includes the following chapter(s).

23 Creating and Managing User Profiles with the Built-in Database

Overview

Purpose

The 8950 AAA Server Management Tool (SMT) provides two ways to manage user profiles: standard RADIUS, text-based user files and a built-in database. The 8950 AAA built-in database is available for managing user profiles and storing accounting records.

The following topics are included in this chapter:

Understanding Database Users

Database Users

> **Important!** This section applies ONLY to the built-in database. If you are using a third-party database, consult the vendor's documentation about creating a database administrative user.

The built-in database, like any other database, requires database manager accounts. In 8950 AAA these are called *Database Users*. When 8950 AAA is first installed there is one Database User account enabled, the System Administrator. The user name for this account is “sa” (System Administrator) and there is no password. The first task of the database

administrator is to assign a password and, if necessary for the site, create additional database user accounts for other people who will manage user profiles or perform database administration tasks.

Important! Database Users are special database managers and administrators and are not the same as the users defined in User Profiles. Database users are those people who will manage the built-in database and manage User Profiles.

Logging in to the Database

Logging into the Database

To launch the Database Tools, click the Database button,  , from the SMT toolbar that appears at the top of the SMT interface. This is available in the row of buttons as displayed in Figure 23-1.

Figure 23-1 SMT-Toolbar

The Database button allows you to launch Database Tools in another process.

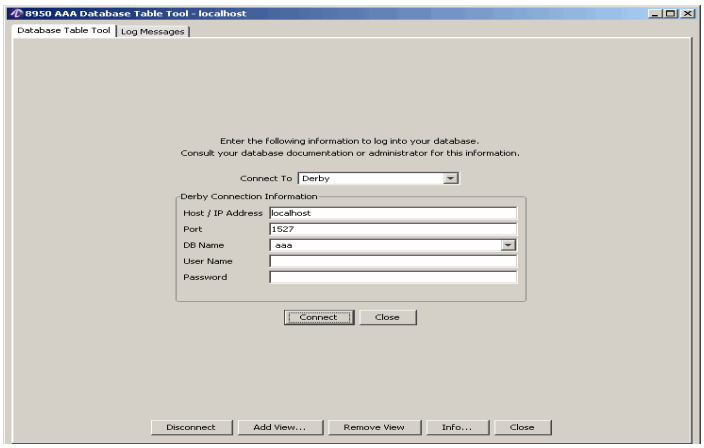
When you click on the Database button you see the following options.

- User Profiles Tool
- Database Table Tool
- Database SQL Tool
- Manage Hypersonic Database Users

You can choose to do perform any of the options that are displayed, by selecting the appropriate option.

The Database Table Tool option allows you to create and manage database user accounts. Select **Database Table Tool...** from the Database options to open this dialog. The Database Table Tool–Login panel appears as shown in Figure 23-2.

Figure 23-2 Database Table Tool-Login panell



Important! The database server is embedded in the 8950 AAA server and starts automatically. Therefore, it is important to remember that in order to manage users, the 8950 AAA server must be running.

The purpose of the Database Table Tool dialog is to allow the database administrator to log in to the database. Use the administrator credentials to login for the first time. You will be able to add a password and add additional database users after you connect.

Creating and Managing User Profiles

Creating and managing User Profiles

A database can be used to hold user profiles. This section discusses use of the built-in 8950 AAA database for creating and managing user profiles for network users.

Important! The Database Table Tool provides access to all tables in the built-in 8950 AAA database. Initially only the User, Accounting and Log views are available. However, if additional views are added, they will also be available in this tool.

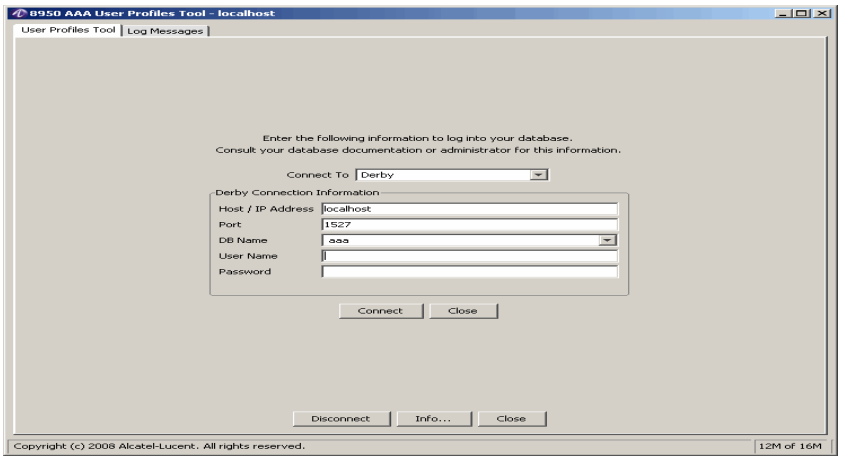
If you are only going to manage user profiles it is recommended that you use the **User Profiles** panel which has support for this function only. Other than being limited to editing user profiles, the User Profiles panel functions is almost the same as the **Database Table Tool**. For your reference, both the User Profiles tool and the Database Table tool are explained in the following sections.

Opening the User Profiles Tool

To open the User Profiles tool:

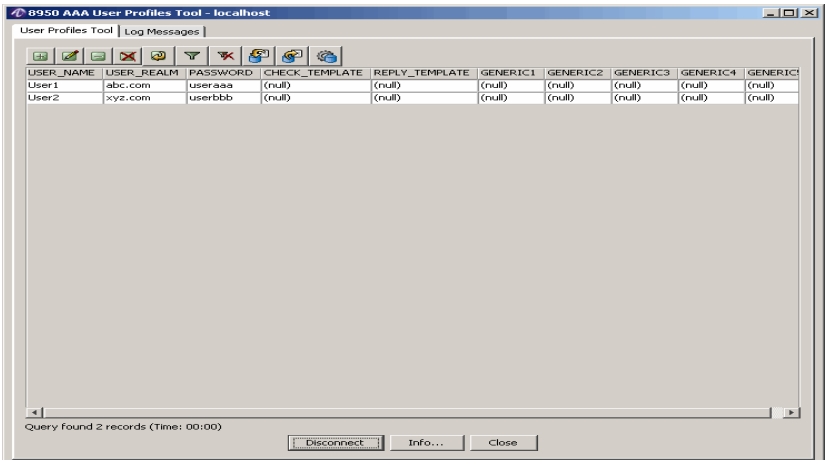
1. Click the Database button and select the **User Profiles Tool...** option. The User Profiles Tool connection panel is displayed, as shown in Figure 23-3.

Figure 23-3 Accessing the User Profiles Tool Panel



2. Select the appropriate **DB Name**, enter a **User Name**, and **Password**.
3. Click **Connect**. The User Profiles Tool–options panel appears as depicted in Figure 23-4.

Figure 23-4 User Profiles Tool Panel-options



Understanding the User Profiles Tool Panel

The User Profiles Tool panel contains the following sections.

- A Table *View*, that is a predefined presentation of data from the User's table. The display area shows data from the table and contains only certain rows or only specific columns. You can edit table contents and manage table views from this panel.
- Contains a set of action buttons in the top of the display area to modify the contents of a table. The function of each button is listed in Table 23-1 on page 7.

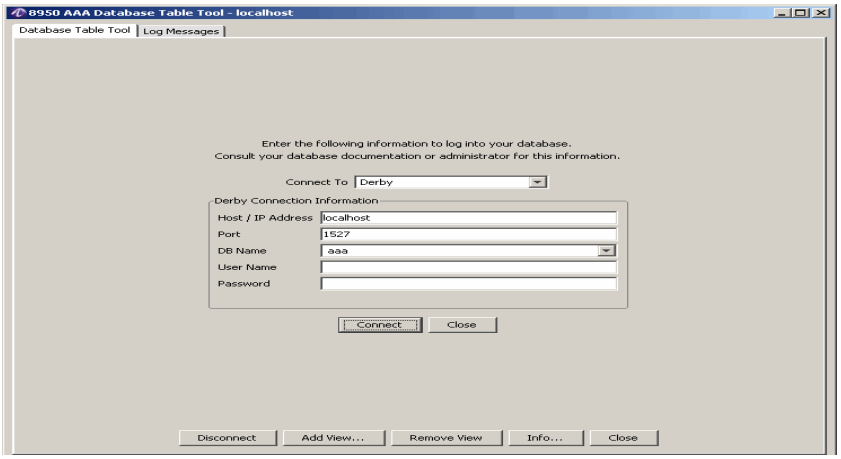
As said earlier, the **User Profiles Tool** is almost the same as the **Database Table Tool**. To try out the actions that can be taken on this panel and to understand more about these functionality, refer to "Understanding the Database Table Tool Panel" on page 6.

Opening the Database Table Tool

To open the database table tool:

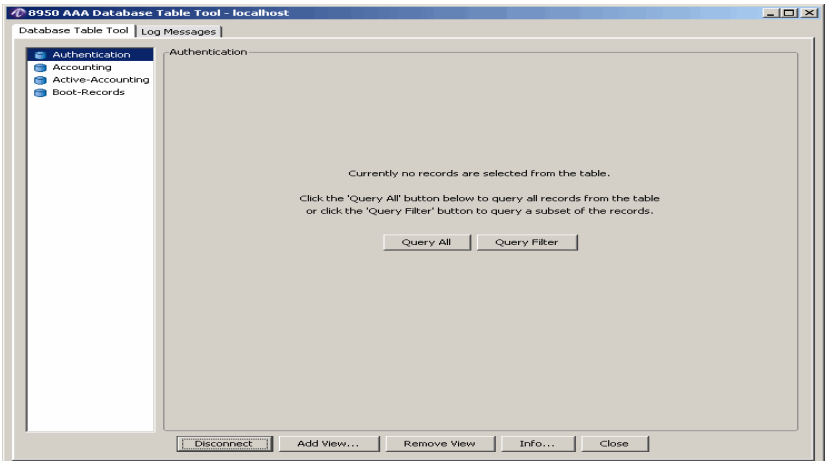
1. Click the Database button and select the **Database Table Tool...** option. The Database Table Tool connection panel is displayed, as shown in Figure 23-5.

Figure 23-5 Accessing the Database Table Tool Panel



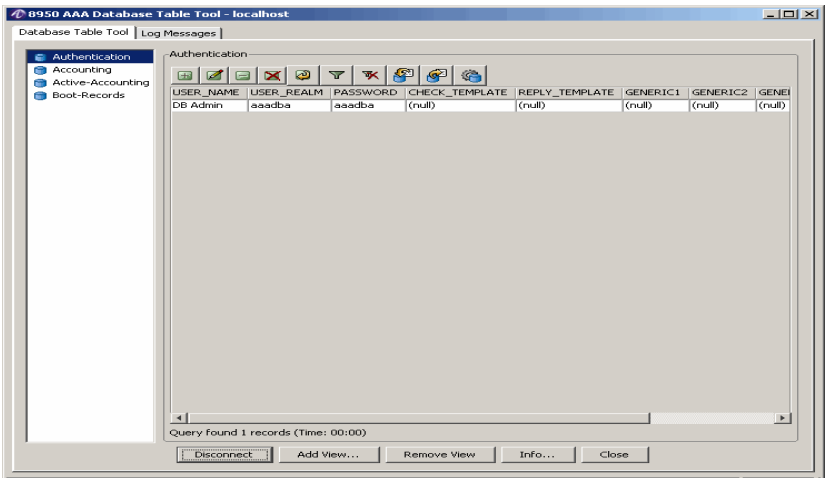
2. Select the appropriate **DB Name**, enter the **User Name**, and **Password**.
3. Click **Connect**. The Database Table Tool–options panel appears as depicted in Figure 23-6.

Figure 23-6 Database Table Tool Panel-options



4. Select the **Database Table Tool** tab and click Query ALL. The Database Table Tool panel appears as depicted in Figure 23-7.

Figure 23-7 Database Table Tool Panel Displaying the Users Table



Understanding the Database Table Tool Panel

The Database Table Tool panel contains the following sections.

- The table view list appears on the left side of the panel and lists the names of all available views.

  Important! The tables that are displayed in the left side of the panel are specific to the users. These are different for each user(s) and are displayed as they are defined in the 8950 AAA database.

  A *Table* is a database file that contains rows of information. Each row in a table represents a record and each row contains one or more columns or fields. The example 8950 AAA supported schema (shown in the following sections) contains 4 tables:

  - *Authentication* for User Profiles
  - *Accounting* for storage of RADIUS accounting records
  - Active-Accounting
  - Boot-Records

A Table *View* is a predefined presentation of data from a table. A view may contain only certain rows or only specific columns. It is possible to have more than one view for a table. For example, one view might list only users in the realm “foo.com” while another view would only list users in “bar.com.” With the SMT *Database Table Tool* you can describe a range of views to help you manage your data. You can edit table contents and manage table views from this panel.

- The display area shows data from the currently selected table and view. Use the action buttons in the top of the display area to modify the contents of a table. The function of each button is listed in Table 23-1.

Table 23-1 Database Table Tool-Action buttons

Name	Description	Icon
Insert	Add a record in the current panel after the selected row. If no row is selected, the record is inserted at the end of the table or list.	
Edit	Edit the values for the selected record.	
Delete	Removes the selected row from the active table or view.	
Delete All	Removes all records from the active table or view	
Copy	Duplicates the selected record. The duplicate record is inserted after the selected record.	
Filter	Define selection criteria to control the records to display.	
Query All	Clears any defined filter criteria and displays/queries all the records.	
Import User File	Import user profiles from a RADIUS text file.	
Export User File	Export user profiles to a comma delimited file.	
Configure Table	Select which columns to use in your User Profiles. Define default filter criteria for displays.	

- Use the control buttons at the bottom of the screen to manage the available table views. They are described in Table 23-2.

Table 23-2 Control Buttons

Name	Description
Disconnect	Disconnect from the database.
Add View	Start the procedure to create a view that will be added to the table view list.
Remove View	Delete a view from the table view list.
Information	Display database information including the database name, database version number, database driver, and database driver version number.
Close	Remove the Database Table Tool panel.

Figure 23-8 Sample Table Showing information

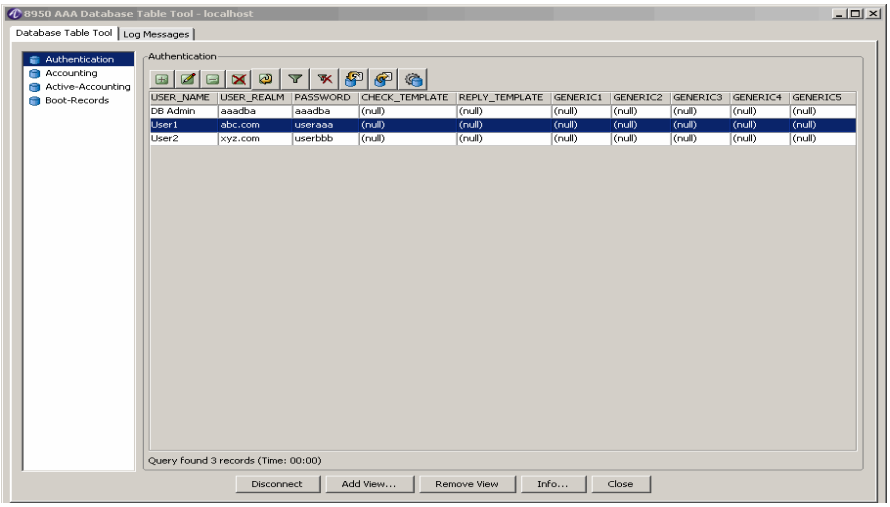


Figure 23-8 shows a table with available fields/information. The check and reply template fields are intended for template names and the generic 1 through 5 fields are for whatever use you desire. Note that the PolicyAssistant does not support use of the generic fields. So, while you may place data into these fields, that data cannot be used in your policies.

8950 AAA supports a predefined database schema for storage of user profiles. However, it is possible for you to edit this schema to remove unneeded columns (fields) and rename fields to more useful settings. When using the PolicyAssistant you may only change the names of the generic fields.

Table Management

The following procedures list steps for creating and managing records within a table.

Panel Modification Buttons are listed in Table 23-1 on page 7.

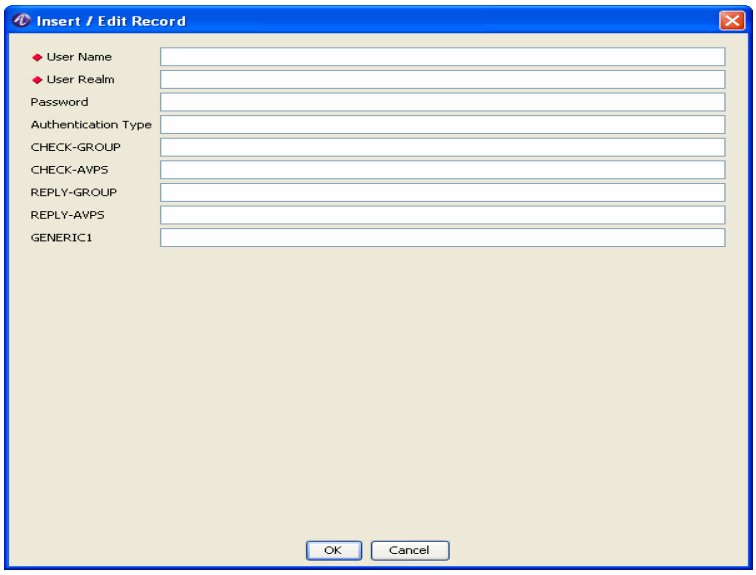
Insert a Record within the Current Panel

To create a new record within the current table, perform the following steps:

1. Click the **Insert** action button.

   Result: The Insert/Edit Record window appears as shown in Figure 23-9.

Figure 23-9 DB Table Too-Insert/Edit Record



2. Enter information into the required fields, **User Name**, **User Realm**. Enter information into the non-required fields as desired.
3. Select **OK** or **Cancel**.

   Click **OK** to accept the new record data. A confirmation prompt appears indicating that the table will be updated.

   Click **Cancel** to reject the new record.

   In either case, return is made to the previous screen.

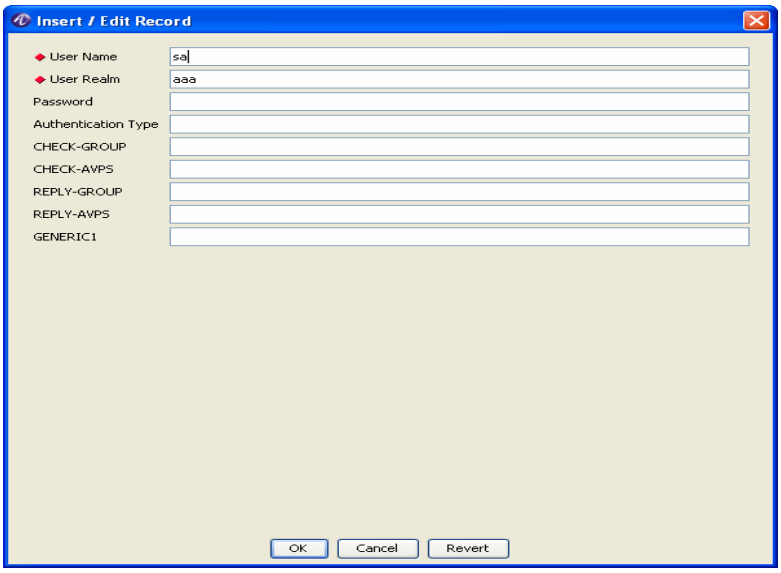
Edit a Record

To edit a record within the current table, perform the following steps:

1. Select the record to edit.
2. Click the **Edit** action button.

   Result: The Insert / Edit Record window appears showing the fields of the selected record as shown in Figure 23-10.

Figure 23-10 DB Table Tool-Selected Record



3. Add or modify information as desired.
4. Select **OK**, **Cancel, or Revert**.

   Click **OK** to accept the modified record data. A confirmation prompt appears indicating that the table will be updated.

   Click **Cancel** to reject the modified record. In either case, return is made to the previous screen.

   Click **Revert** to undo the modifications that have not been saved.

   After selecting OK or Cancel, return is made to the previous screen; after selecting Revert, the Insert/Edit Record window continues to be displayed.

Delete a Record

To delete a record within the current table, perform the following steps:

1. Select the record to delete.
2. Click the **Delete** action button.

   Result: The selected record is deleted from the current table.

   Important! There is no operation to undo the record deletion.

Delete All Records

To delete all records within the current table, perform the following steps:

1. Click the **Delete All** action button.

   Result: A confirmation window appears, as displayed in Figure 23-11.

Figure 23-11 DB Table Tool-Delete All Records Confirmation

2. Select **Yes** to delete all records or **No** to cancel the request.

Copy Records

This procedure allows you to use an existing record as a template for a new record within the current table. It is required that the new record is unique; therefore, you must modify at least one of the required fields (User Name, User Realm) before creating the new record. The steps of the procedure are as follows:

1. Select the record to copy.
2. Click the **Copy** action button.

   Result: The Insert / Edit Record window appears as shown in Figure 23-10.

3. Modify at least one of the required fields to insure the uniqueness of the new record. Modify any of the non-required fields as desired.
4. Select **OK**, **Cancel, or Revert**.

   Click **OK** to accept the modified record data. A confirmation prompt appears indicating that the table will be updated.

   Click **Cancel** to reject the modified record. In either case, return is made to the previous screen.

   Click **Revert** to undo the modifications that have not been saved.

   After selecting OK or Cancel, return is made to the previous screen; after selecting Revert, the Insert/Edit Record window continues to be displayed.

Filter Records

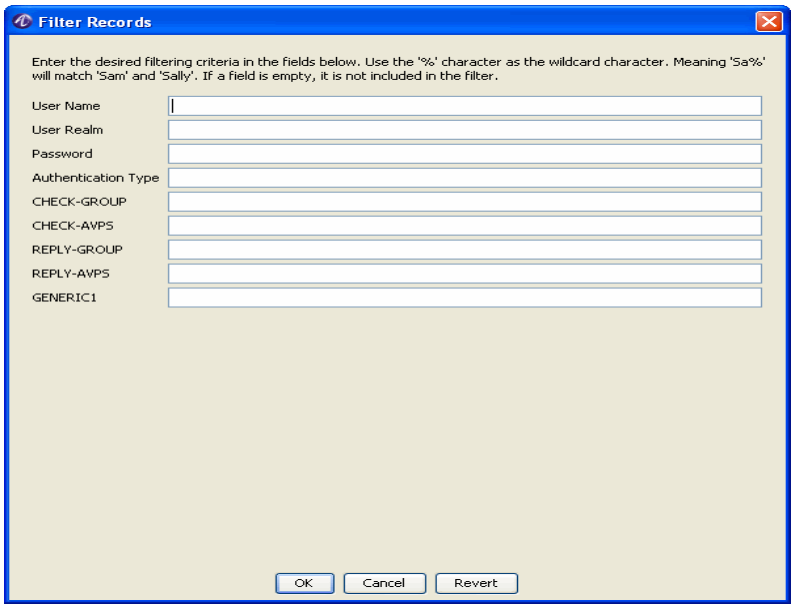
This procedure allows you to query records from the current table using a defined set of criteria. After the query is performed, resulting records are displayed. This command customizes the view of the records; it does not delete records. To disable the filter, click the **Query all records** action button.

The steps of the procedure are as follows:

1. Click the **Filter** action button.

   Result: The Filter Records window appears as shown in Figure 23-12.

Figure 23-12 DB Table Tool-Filter Records



2. Enter data within the fields of the Filter Records window to create filtering criteria. The data will be used for a record search by matching field values within the existing table.
3. Select **OK**, **Cancel, or Revert**.

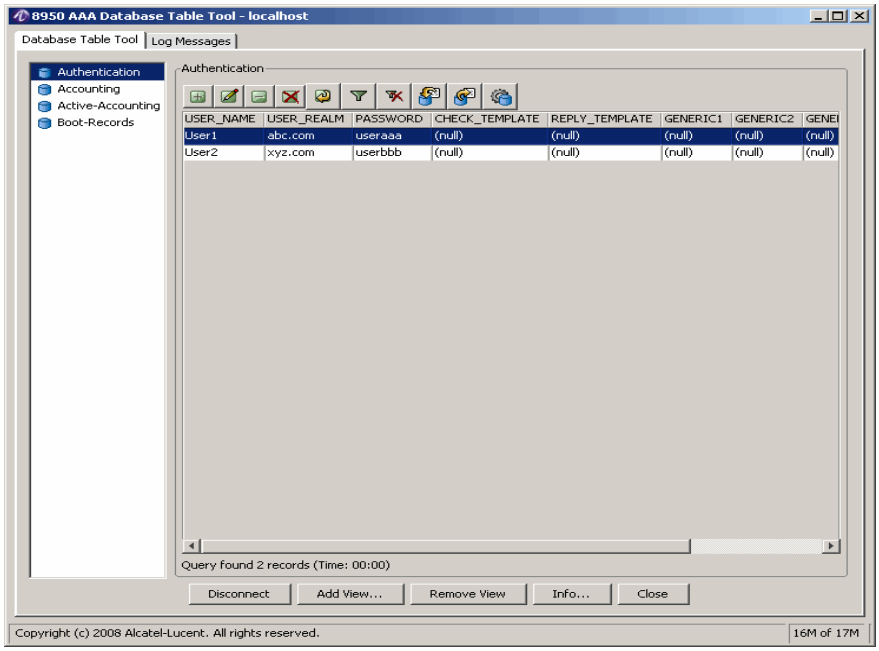
   Click **OK** to accept the filter. Return is made to the new table view.

   Click **Cancel** to reject the filter. The original table view is displayed.

   Click **Revert** to undo modifications that have not been saved. This allows you to re-enter data.

After clicking **OK**, the table view appears as shown in Figure 23-13.

Figure 23-13 Sample Filter Results



Clear a Filter and Query all records

To disable the current filter, perform the following steps:

1. Click the **Query all records** action button.

   Result: The table with its original set of records appears.

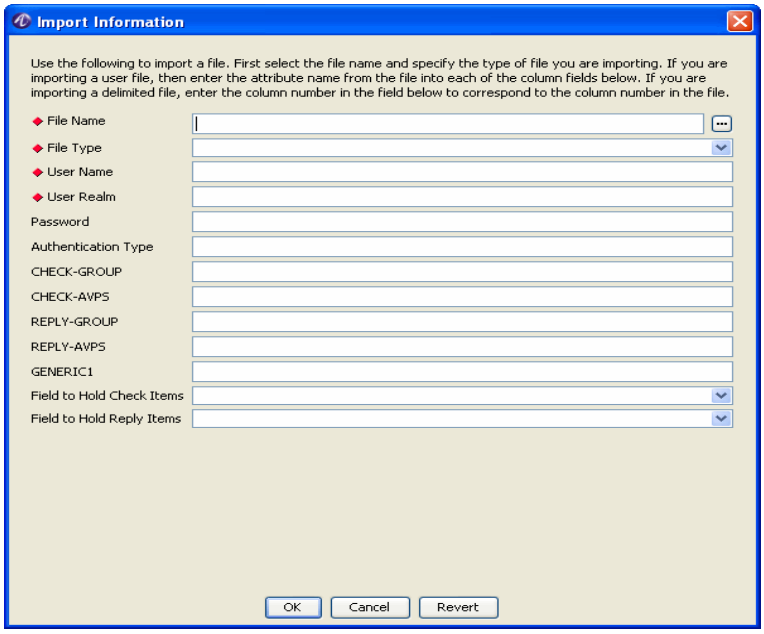
Import User File

This procedure allows you to copy data from a file to a new record within the current table. The steps of the procedure are as follows:

1. Click the **Import User File** action button.

   Result: The Import Information window appears as shown in Figure 23-14.

Figure 23-14 DB Table Tool-Import Information

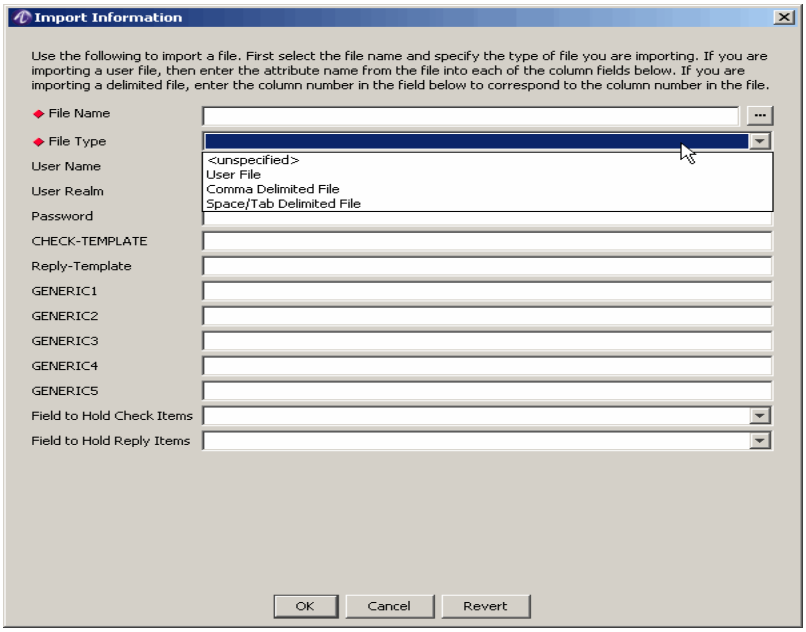


2. Enter data in the required fields.

   File Name requires an absolute directory path that may be typed within the field or selected using the browse button that follows the field.

   Set the value of **File Type** by choosing one of the list items of this field, as shown in Figure 23-15. EnterIf you intend to import a user file, then enter the attribute name from the file into each of the column fields. If you wish to import a delimited file, enter the column number in the field to correspond to the column number in the file.

Figure 23-15 DB Table Tool-File Type List



Set the values of User Name and User Realm.

3. Select **OK**, **Cancel**, or **Revert**.

   Click **OK** to accept the modified record data. A confirmation prompt appears indicating that the table will be updated.

   Click **Cancel** to reject the modified record.

   Click **Revert** to undo the modifications that have not been saved.

   After selecting OK or Cancel, return is made to the previous screen; after selecting Revert, the Import Information window continues to be displayed.

Configure a Table

This procedure allows you to control the configuration of the current table. Configuration elements include:

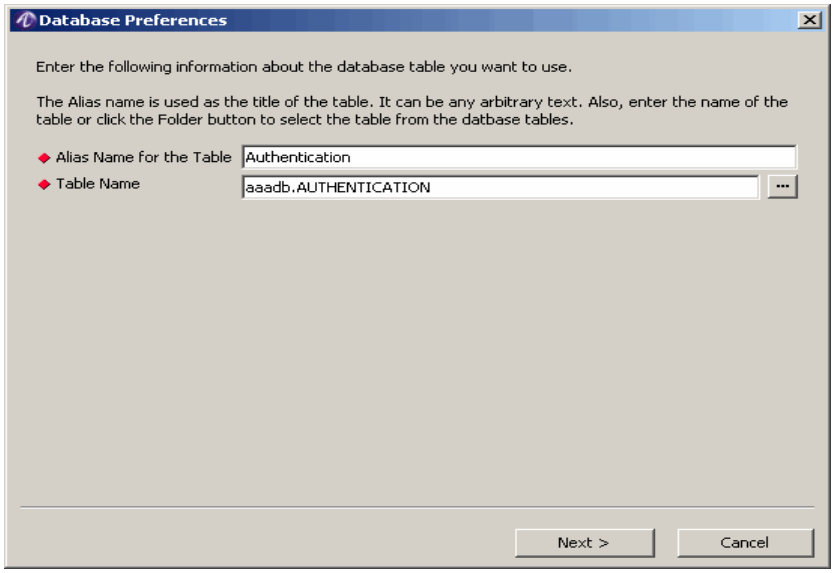
- Alias name of the table
- Table name
- Columns that are displayed
- Automatic initialization of table fields
- Initial table filter
- Sorting criteria

The steps of the procedure are as follows:

1. Click the **Table Configuration Options** action button.

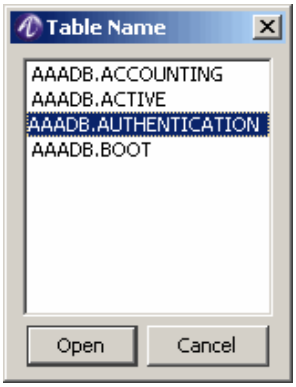
   Result: The Database Preferences window appears as shown in Figure 23-16.

Figure 23-16 Database Preferences-Alias and Table Names



Enter the Alias Name and the Table Name for the table. You may select a Table Name by clicking the folder button that appears after the Table Name field. In this case, a list of allowable table names is displayed as shown in Figure 23-17. Select the Table Name and click the Open button.

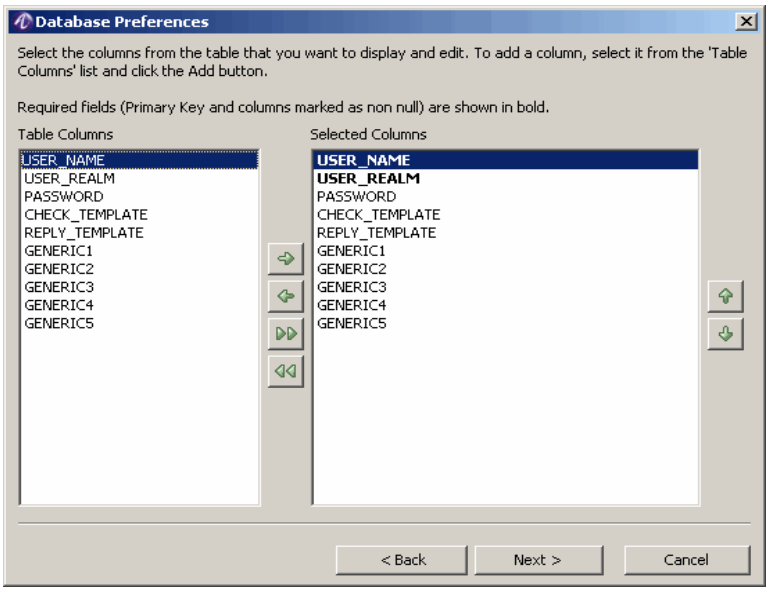
Figure 23-17 Database Preferences-Table Names



When done, click **Next** on the Database Preferences window.

Result: The Database Preferences window appears as shown in Figure 23-18.

Figure 23-18 Database Preferences-Selected Columns



2. Use this window to determine the table columns to be displayed. To do this, select a name from the Table Columns list and click the **Add** button . The name appears within the Selected Columns list.

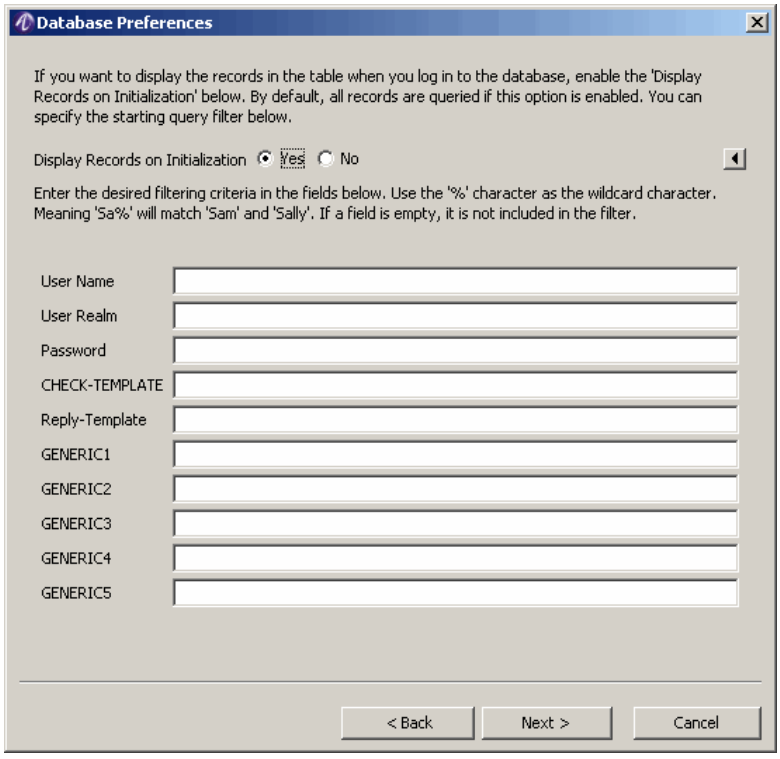
   To select all table columns, click the **Add All** button .

   Bold Table Column names indicate columns that are required.

   When done, click **Next** on the Database Preferences window.

   Result: The Database Preferences window appears as shown in Figure 23-19.

Figure 23-19 Database Preferences-Initialization and Filter



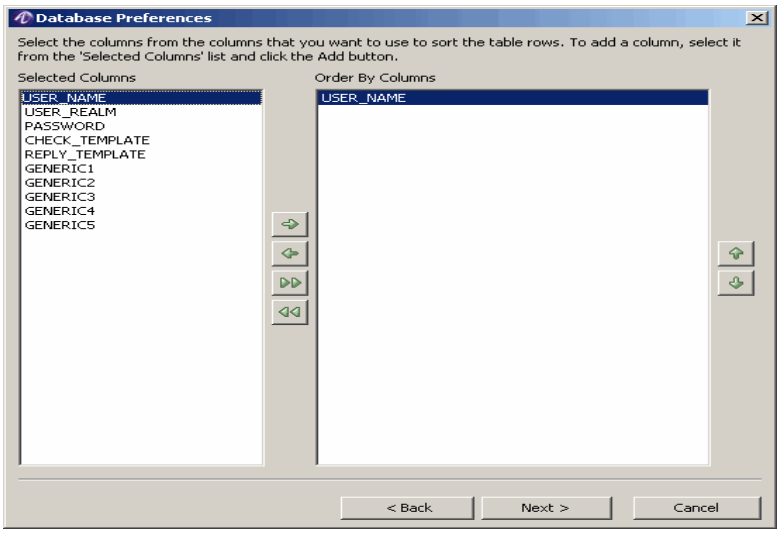
3. The **Display Records on Initialization** is disabled by default. Select the **Yes** (Enable) button. This ensures that all records are queried and displayed as soon as you login to the database. To prevent the display, disable the checkbox by selecting **No**.

   The remaining fields on this window allow you to create a filter that is used for the initial display of table records. For information on filtering, refer to "Filter Records" on page 11.

   When done, click **Next** on the Database Preferences window.

   Result: The Database Preferences window appears as shown in Figure 23-20.

Figure 23-20 Database Preferences-Sorting



4. Use this window to customize the current table by sorting the rows as desired. To do this, select a name from the Selected Columns list and click the **Add** button. The name appears within the Order By Columns list.

   To select all table columns, click the **Add All** button.

   To reorder the Order By Columns list, select an item to move within the list and click the **Move Up** button or click the **Move Down** button.

   To delete all records, click the **Delete all records**.

   When done, click **Next** on the Database Preferences window.

   Result: The Database Preferences window appears with a message stating that the procedure is complete.

5. Click **Finish** to return to the Database Table Tool panel or click **Back** to return to the previous window.

Understanding Database SQL Tool

Using the Database SQL Tool

The database SQL Tool can be used to run SQL commands and get required results. This section discusses the use of the built-in 8950 AAA SQL database tool for running and managing queries of the network users.

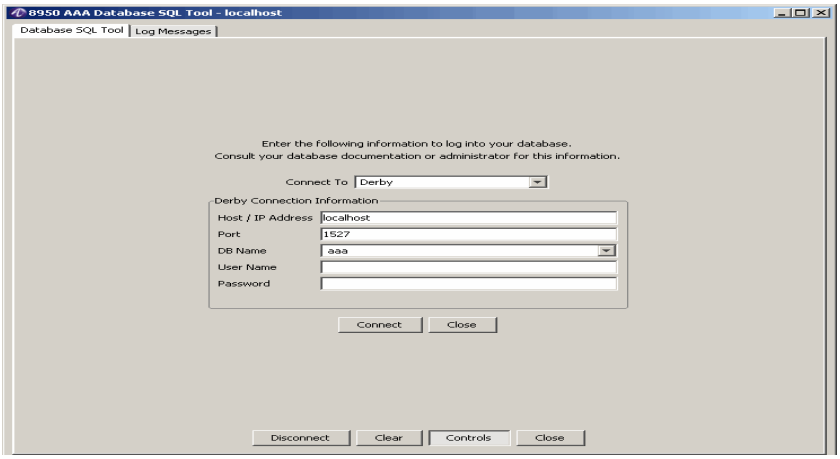
Important! The Database SQL Tool provides access to all tables in the built-in 8950 AAA database.

Opening the Database SQL Tool

To open the Database SQL tool:

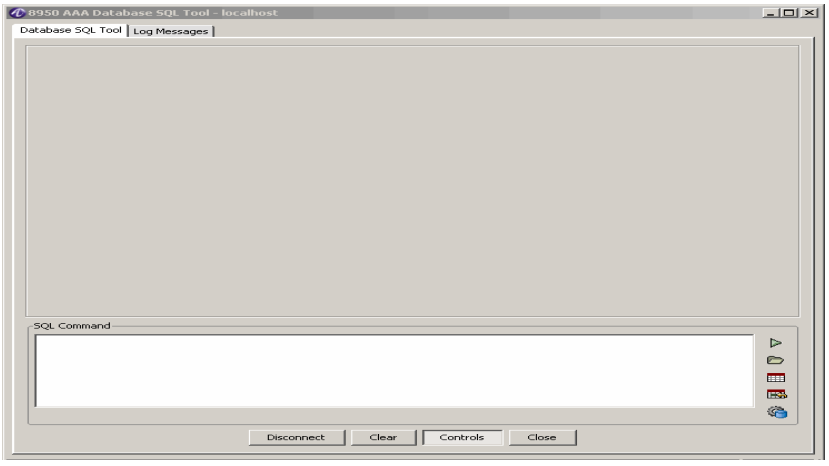
1. Click the Database button and select the **Database SQL Tool...** option. The Database SQL Tool connection panel is displayed, as shown in Figure 23-21.

Figure 23-21 Accessing the Database SQL Tool Panel



2. Select the appropriate **DB Name**, enter a **User Name**, and **Password**.
3. Click **Connect**. The Database SQL Tool–Blank screen panel is displayed as shown in Figure 23-22.

Figure 23-22 Database SQL Tool Panel-Blank screen



Important! The display area will be blank as no data is selected or no SQL command is executed. Use the action buttons in the right side of the SQL Command

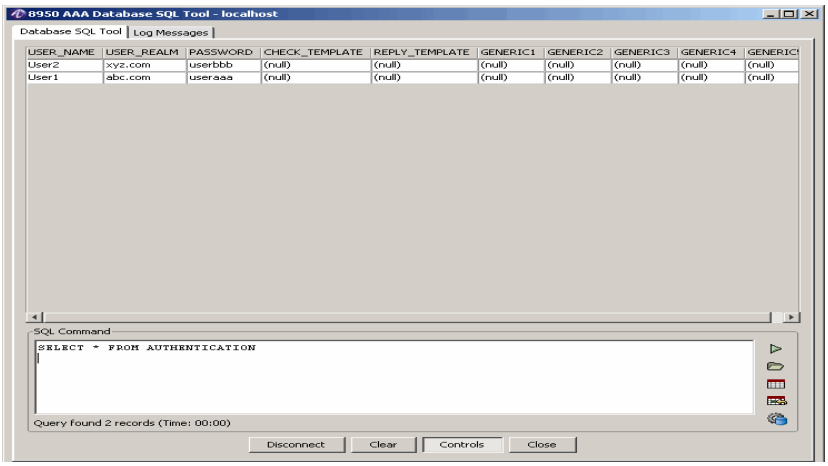
area to execute the required commands. The function of each of these buttons are listed in Table 23-3.

Table 23-3 Database SQL Tool Panel-Action buttons

Name	Description	Icon
Execute Command	Executes the SQL command that is typed in the SQL Command area of the Database SQL Tool panel. The shortcut key F4 can also be used to execute the command.	
Open Script File	Displays a list of available Configuration files in the database. Select the required file and click Open.	
Database Tables	Displays the list of available tables in the database. Select the required table and click Select.	
Database Fields	Displays the list of available tables and the fields corresponding to those tables in the database. Select the required table and fields and click Select.	
History of Commands	Displays the list of commands executed. Select the required command and click Select to repeat the execution of the same command.	

4. Enter any SQL command that you like and click on the Execute Command button. When a SQL command, as shown in Figure 23-23, is provided in the Database SQL Tool panel and executed, appropriate values are displayed as shown in the Database SQL Tool panel as shown in Figure 23-23.

Figure 23-23 Database SQL Tool Panel



5. Use the control buttons at the bottom of the screen to manage the available table views. They are described in Table 23-4.

Table 23-4 Database SQL Tool panel-Control buttons

Name	Description
Disconnect	Disconnects from the database.
Clear	Clears the Database SQL Tool panel.
Control	Displays or hides the action buttons and SQL Command window from the view list.
Close	Removes the Database Table Tool panel.

Managing Hypersonic Database Users

About Managing Hypersonic database users

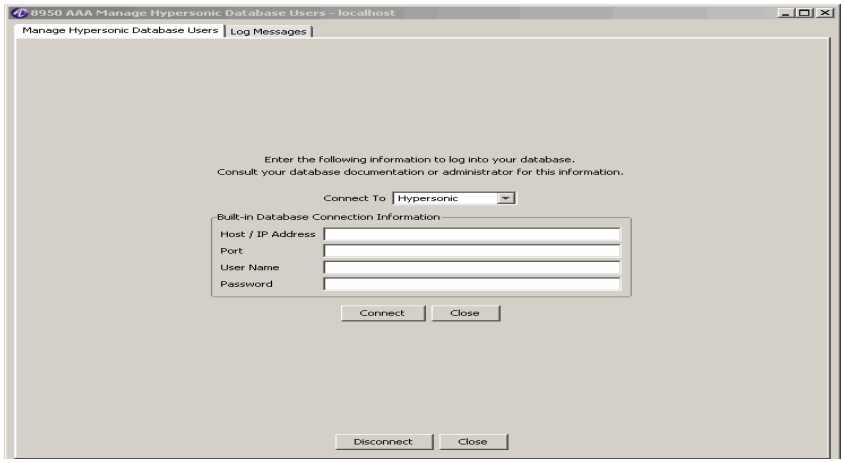
As pexplained earlier, a database is used to hold different type of user profiles. This section discusses use of the Hypersonic database for creating and managing user profiles for network users.

Opening the Hypersonic Database Users Tool

To open the database table tool:

1. Click the Database button and select the **Manage Hypersonic Database Users...** option. The Manage Hypersonic Database Users connection panel is displayed, as shown in Figure 23-24.

Figure 23-24 Manage Hypersonic Database Users connection Panel



2. Specify appropriate **Host / IP Address**, **Port**, **User Name**, and **Password**.
3. Click **Connect** to go to the Hypersonic Database Users Tool panel.

Important! The Hypersonic Database Users Tool is almost the same as the **Database Table Tool**. For more information, refer to "Understanding the Database Table Tool Panel" on page 6.

END OF STEPS

Part VII: Other chapters

Overview

Purpose

This part contains the other chapters related to SMT.

Contents

This part includes the following chapter(s).

24 Server Diagnostics and Control Commands

Overview

Purpose

This chapter discusses the use of server diagnostics with the 8950 AAA server. It also describes the control command set.

The following topics are included in this chapter:

Server Diagnostics and Control

Server diagnostics and control

As described in Chapter 18, “Using LiveAdministrator,” access is available to the administrator interface through the LiveAdministrator panel of the Server Management Tool. From the LiveAdministrator panel, click the **Advanced** option to access the RADIUS and state server commands. You can also use a Telnet session or the Command plug-in within PolicyFlow to issue commands.

Refer to the appropriate help topics in the SMT for more information about issuing commands from within the LiveAdministrator panel, from a Telnet session, or the Command plug-in.

> **Important!** Universal State Server commands are combined with the 8950 AAA server commands

List of Server Commands

About Server Commands

This section describes each command by listing the following components:

- Command name
- Brief description of the command
- Command format containing syntax and arguments
- Table of arguments, if any

Argument description

The following list describes the special symbols used within the command format line of each description.

- Arguments within square brackets ([ ]) are optional.
- Arguments within angle brackets (< >) are variables that represent an appropriate value.
- Arguments separated by a pipe symbol (|) indicate that only one of the arguments can be used for each execution of the command.

cache

The cache command is used to add, count, delete, or list a cache entry.

Command Format:

`cache add KEY[NAME=VALUE][NAME=VALUE]...|count KEY|delete KEY|list KEY|dump KEY|save FILE|load FILE`

The following][section lists the **cache** commands and their arguments:

cache add

Description: Adds an entry to the cache.

Command Format: **`cache add [-live <sec>][-idle<sec>] <key> [NAME-VALUE]`**

-live <sec>	The amount of time, in seconds, for this entry to reinforce the `-live`.
-idle <sec>	The amount of time, in seconds, to remove the entry from the cache if the entry has not been updated.
key	The name of the cache entry.
NAME-VALUE	A list of attribute=value pairs.

cache count

Description: Counts entries matching the key (may use trailing wild cards).

Command Format: **`cache count <key>`**

<*key*>	The key that matches the count entries.

cache delete

Description: Deletes entries matching the key (may use trailing wild cards).

Command Format: **`cache delete <key>`**

<*key*>	The key that matches the entries to be deleted.

cache dump

Description: Dumps entries matching the key (may use trailing wild cards).

Command Format: **`cache dump <key>`**

<*key*>	The key that matches the entries to be dumped.

cache list

Description: Lists entries matching the key (may use trailing wild cards).

Command Format: **`cache list <key>`**

<*key*>	The key that matches the entries to be listed.

cache load

Description: Loads the cache contents from a file.

Command Format: **`cache load <fileName>`**

<*filename*>	The name of the file from which cache contents will be extracted.

cache names

Description: List cache names.

Command Format: **`cache`**

There are no arguments for this command.

cache save

Description: Saves the cache contents to a file.

Command Format: **`cache save <fileName>`**

<*filename*>	The name of the file in which cache contents will be saved.

client

This section list the **client** commands and the argument:

client classes

Description: Lists the client classes.

Command Format: **`client classes`**

There are no arguments for this command.

derby

The following section lists the derby commands and their arguments.

derby backup

Description: Backup for an internal derby database.

Command Format: **`derby backup <database> [<directory>]`**

<*database*>	Name of the database.
<*directory*>	Name of the directory.

derby connect

Description: Connect to derby database.

Command Format: **`derby connect <database>`**

<*database*>	Name of the database.

derby create

Description: Creates an internal derby database.

Command Format: **`derby create <database>`**

<*database*>	Name of the database.

derby disconnect

Description: Disconnect from a derby database.

Command Format: **`derby disconnect`**

There are no arguments for this command.

derby exec

Description: Executes a SQL statement against a connected database.

Command Format: **derby create {<statement-element>}**

<*statement-element*> The SQL statement.

derby freeze

Description: Freezes an internal derby database.

Command Format: **derby freeze <database>**

<*database*> Name of the database.

derby info

Description: Lists some metadata for the currently open connection.

Command Format: **derby info**

There are no arguments for this command.

derby list

Description: Lists internal derby databases.

Command Format: **derby list [<database> <timestamp>]**

<*database*> Name of the database.

<*timestamp*> Enter the timestamp (yyyy-mm-dd hh:mm:ss[nnnnnn].

derby login

Description: Cache security credentials for derby access.

Command Format: **derby <username> <password>**

<*username*> Login user name.

<*password*> Login password.

derby info

Description: Uncache security credentials for derby access.

Command Format: **derby logout**

There are no arguments for this command.

derby restore

Description: Restores aa internal derby database.

Command Format: **derby restore <database> (<timestamp|<directory>)**

<*database*>	Name of the database.
<*timestamp*>	Enter the timestamp (yyyy-mm-dd hh:mm:ss[nnnnnn].
<*directory*>	Name of the directory.

derby run

Description: Runs a script file against a connected database.

Command Format: **derby run <filename>**

<*filename*>	Name of the file.

derby unfreeze

Description: Unfreezes an internal derby database.

Command Format: **derby unfreeze <database>**

<*database*>	Name of the database.

diag

This command runs diagnostics.

Command Format: **diag chrono [dump | list] | engine [active|state|stats] | fuse list | method stats | normal [list | stats] | queue [list | reset | resetstats]**

diag atfile dump

Description: Dumps the AtFileProperty Informations.

Command Format: **diag atfile dump [file [method [property]]]**

<*file*>	Name of the file.
method	Name of the method
property	Name of the property

diag bufferpool stats

Description: Displays buffer pool statistics.

Command Format: **diag buferpool stats**

There are no arguments for this command.

diag chrono

The following section lists the diag chrono commands and their arguments.

diag chrono dump

Description: Dumps the chronograph entries (hi resolution timers).

Command Format: **`diag chrono dump`**

There are no arguments for this command.

Example:

```
==> diag chrono dump
Ok.
==>
```

diag chrono kick

Description: Kicks the chronograph timer thread (paranoia).

Command Format: **`diag chrono kick`**

There are no arguments for this command.

diag chrono list

Description: Lists the chronograph entries (hi res timers).

Command Format: **`diag chrono list`**

There are no arguments for this command.

diag engine

The following section lists the diag engine commands and their arguments:

diag engine active

Description: Dumps the engine active table (duplicates).

Command Format: **`diag engine active [log]`**

`[log]`	The name of the log.

diag engine state

Description: Dumps the engine state table (outstanding challenges/continues).

Command Format: **`diag engine state`**

There are no arguments for this command.

diag engine stats

Description: Lists the engine statistics.

Command Format: **`diag engine stats`**

There are no arguments for this command.

diag field

The following section lists the diag field commands and their arguments:

diag field list

Description: Lists the field entries.

Command Format: **`diag field list`**

There are no arguments for this command.

diag field stats

Description: Lists the field statistics.

Command Format: **`diag field stats`**

There are no arguments for this command.

diag fuse

The following section lists the diag fuse commands and their arguments:

diag fuse list

Description: Lists the fuse entries (lo res timers).

Command Format: **`diag fuse list`**

There are no arguments for this command.

diag method

The following section lists the diag method commands and their arguments:

diag method stats

Description: Lists the method statistics.

Command Format: **`diag method stats [-notrim]`**
`[-sort][<flow>] [-<method>] [-<disposition>] [-<bucket>]]]`
`<flow> ::= * | auth | acct`
`<method> :: = * | <methodName>`

<disposition> :: = * | total | expire| statetimeout | <dipositionName>
<bucket> :: = * | count | time

[-notrim]	Specifies to include all statistics. When not specified, only statistics with non-zero values are retrieved.
[-sort]	Specifies to sort the statistics by key name
[<flow>[<-	Narrows the methods to view. **<flow>** specifies which PolicyFlow to view **(*, auth, or acct).**
[<-<method>]	Specifies which method name to view (* or specific PolicyFlow method name. This attribute may be expressed as `*` or **<**`methodName`**>** .
[-<disposition>]	Specifies which statistic item to view. This attribute may be expressed as: `Total`, **Success, Failure, Error, Accept, Reject, Discard, Suspend, Jump, Challenge, Continue, Expire, and StateTimeout).**
[-<bucket>]	Specifies either TIME or COUNT. This parameter may be expressed as `*`, `count`, or `time`.

diag normal

The following section lists the diag normal commands and their arguments:

diag normal list

Description: Lists the normalized list.

Command Format: **diag normal list**

There are no arguments for this command.

diag normal stats

Description: Lists the normalized list statistics.

Command Format: **diag normal stats**

There are no arguments for this command.

diag pending

The following section lists the diag pending commands and their arguments:

diag pending stats

Description: Lists the pending statistics for a server.

Command Format: **`diag pending stats`**

There are no arguments for this command.

diag queue

The following section lists the diag queue commands and their arguments:

diag queue list

Description: Lists the queues.

Command Format: **`diag queue list`**

There are no arguments for this command.

diag queue reset

Description: Resets the queue content.

Command Format: **`diag queue reset [<queueName>]`**

[<queueName>] The name of the queue.

diag queue resetstats

Description: Resets the queue statistics.

Command Format: **`diag queue resetstats [<queueName>]`**

[<queueName>] The name of the queue.

diag tal

The following section lists the diag TAL commands and their arguments:

diag tal literal dump

Description: Dumps the TAL literal cache.

Command Format: **`diag tal literal dump`**

There are no arguments for this command.

diag tcp

The following section lists the diag tcp commands and their arguments:

diag tcp keys

Description: Dumps the current selector keys.

Command Format: **`diag tcp keys`**

There are no arguments for this command.

diag tcp stats

Description: Dumps the tcp stats.

Command Format: **`diag tcp stats`**

There are no arguments for this command.

diag watch

The following section lists the diag watch commands and their arguments:

diag watch list

Description: Lists the chronograph entries (hi res timers).

Command Format: **`diag watch list`**

There are no arguments for this command.

diameter

The following section lists the diameter commands and their arguments:

diameter route list

Description: Lists the diameter routes.

Command Format: **`diameter route list`**

There are no arguments for this command.

eap aka cache

The following section lists the eap aka cache commands and their arguments:

eap aka cache count

Description: Counts fast reauth entries by permanent username.

Command Format: **`eap aka cache count[<permanent_user_name>]`**

[<permanent_user_nam e>]	The name of the permanent user.

eap aka cache delete

Description: Deletes fast reauth entries by permanent username.

Command Format: **`eap aka cache delete [<permanent_user_name>]`**

[<permanent_user_nam e>]	The name of the permanent user.

eap aka cache list

Description: Lists fast reauth entries by permanent username.

Command Format: **`eap aka cache listt[<permanent_user_name>]`**

[<permanent_user_nam e>]	The name of the permanent user.

eap aka cache

The following section lists the eap sim cache commands and their arguments:

eap sim cache count

Description: Counts fast reauth entries by permanent username.

Command Format: **`eap sim cache count[<permanent_user_name>]`**

[<permanent_user_nam e>]	The name of the permanent user.

eap sim cache delete

Description: Deletes fast reauth entries by permanent username.

Command Format: **`eap sim cache delete [<permanent_user_name>]`**

[<permanent_user_nam e>]	The name of the permanent user.

eap sim cache list

Description: Lists fast reauth entries by permanent username.

Command Format: **`eap sim cache listt[<permanent_user_name>`**]

[<permanent_user_nam e>]	The name of the permanent user.

file

This command manages file behavior.

Command Format:

file close <filename>|delete <filename>|list|open|reload {<filename>}|rename <oldfilename> <newfilename>|view <filename>

The following section lists the **file** commands and their arguments:

file close

Description: Closes a file.

Command Format: **file close <fileName>**

<*fileName*> The name of file to be closed.

file delete

Description: Deletes a file.

Command Format: **file delete <fileName>**

<*fileName*> The name of file to be deleted.

file list

Description: Lists files in the run directory.

Command Format: **file list**

There are no arguments for this command.

file open

Description: Opens files.

Command Format: **file open**

There are no arguments for this command.

file reload

Description: Reloads file(s) or list files that can be reloaded.

Command Format: **file reload**

<*fileName*> The name of the file to be reloaded.

file rename

Description: Renames a file.

Command Format: **`file rename <oldFileName> <newFileName>`**

<oldFileName>	The current name of the file to be renamed.
<newFileName>	The new name of the file to be renamed.

file view

Description: Views the contents of a file.

Command Format: **`file view <fileName>`**

<fileName>	The name of the file to be viewed.

help

The Help command lists and describes all the commands that can be used with SMT (Server Management Tool). These commands are listed in this chapter.

Command Format: **`help [CMD]`**

[CMD]	Replace this argument with a command name to display the command usage.

ipam

The following section lists the ipam commands and their arguments:

ipam lease

Description: Displays ipam leases matching the given IP address

Command Format: **`ipam lease [selector] <address>`**

address	Leased IP address

ipam pool

Description: Dumps ipam pool prefixes

Command Format: **`ipam pool <pool name> <all|used|free> [filename]`**

poolname	Name of the pool.
all|used|free	Mention all, used, or free pools.

java

This command inquires into the status of the java virtual machine.

Command Format: **`java gc|memory|properties|threads|version`**

The following section lists the **java** commands and their arguments:

java gc

Description: Forces a garbage collection on the JVM.

Command Format: **`jave gc`**

There are no arguments for this command.

java gc stats

Description: Lists the JVM garbage collector statistics.

Command Format: **`jave gc stats`**

There are no arguments for this command.

java memory

Description: Lists JVM memory statistics.

Command Format: **`java memory`**

There are no arguments for this command.

java properties

Description: Lists java properties

Command Format: **`java properties`**

<*fileName*> The name of the file to display java properties.

java thread dump

Description: Displays java lock information.

Command Format: **`java thread locks[all]`**

There are no arguments for this command.

java thread locks

Description: List stack traces for all threads.

Command Format: **`java thread dump`**

There are no arguments for this command.

java thread monitor contention

Description: Controls java thread contention monitoring.

Command Format: **`java thread monitor contention [<boolean>`**]

<*boolean*> Mention true or false.

java thread monitor cpu

Description: Controls java thread cpu time monitoring.

Command Format: **`java thread monitor cpu [<boolean>]`**

<*boolean*>	Mention true or false.

java thread stats

Description: Lists thread statistics.

Command Format: **`java thread stats`**

There are no arguments for this command.

java threads

Description: Lists JVM threads.

Command Format: **`java threads`**

There are no arguments for this command.

java version

Description: Lists JVM version.

Command Format: **`java version`**

There are no arguments for this command.

login

This command establishes identity.

Description: Establishes identity.

Command Format: **`login <username> <password>`**

<*username*>	The name to be used for the user.
<*password*>	The protected, “secret,” word to access the system.

logrule

This command controls logging and rollover file cache.

The following section lists the **logrule** commands and their arguments:

logrule add

Description: Adds a logging rule.

Command Format: **`logrule add <rule>`**

<rule> ::= [<areaCondition>] [<itemCondition>] [<logLevel>] [<pattern>] {<channel>}

[<areaCondition>]::= AREA=<wildcarad value>

[<itemCondition>]::= <variable expression> =<wildcard value>.

<rule> ::= [<areaCondition>] [<itemCondition>] [<logLevel>] [<pattern>] {<channel>}	Specifies the section of the 8950 AAA server where the message is generated. **rule may be expressed as areaCondition, itemCondition, logLevel, pattern, or channel.**
<areaCondition>:= AREA=<wildcarad value>	areaCondition may be expressed as **AREA=<wildcard value>.**
<itemCondition>::= <variable expression> =<wildcard value>	Specifies an expression to match attributes and values. itemCondition may be expressed as **<variable expression> =<wildcard value>**.

logrule areas

Description: Lists available areas.

Command Format: **logrule areas**

There are no arguments for this command.

logrule clear

Description: Clears all logging rules.

Command Format: **logrule clear**

There are no arguments for this command.

logrule delete

Description: Deletes a logging rule.

Command Format: **logrule delete <num>**

<num>	The log rule number to be deleted.

logrule insert

Description: Inserts a logging rule.

Command Format: **logrule insert <num> <rule>**

<num> <rule> ::= [<areaCondition>] [<itemCondition>] [<logLevel>] [<pattern>] {<channel>}

[<areaCondition>]::= AREA=<wildcard value>

[<itemCondition>]::= <variable expression> =<wildcard value>

<num>	Specifies where to insert this log rule.
<rule> ::= [<areaCondition>] [<itemCondition>] [<logLevel>] [<pattern>] {<channel>}	rule may be expressed as **areaCondition, itemCondition, logLevel, pattern, or channel**.
[<itemCondition>]::= <variable expression> =<wildcard value>	**itemCondition may be expressed as a variable expression, or a wildcard value**.

logrule list

Description: Lists logging rules.

Command Format: **logrule list**

There are no arguments for this command.

Example:

```
==> logrule list
1  area   *  INFO   <ALL>  LogToFile
==>
```

logrule load

Description: Loads logging rules from a file.

Command Format: **logrule load <fileName>**

<fileName>	The name of the file from which the logging rules will be loaded.

logrule move

Description: Moves a logging rule.

Command Format: **logrule move <num> <num>**

numb	The start and end logging rule numbers to be moved.

logrule remove

Description: Deletes a logging rule.

Command Format: **`logrule remove <num>`**

<num>	The number of the log rule to be deleted.

logrule save

Description: Dumps logging rules to a file.

Command Format: **`logrule save <fileName>`**

<fileName>	The name of the file to which the logging rules will be dumped.

logrule swap

Description: Swaps two logging rules.

Command Format: **`logrule swap <num> <num>`**

numb	The number of the two rules to be swapped with one another.

peer

The following section lists the peer commands and their arguments:

peer auto

Description: Sets peer auto.

Command Format: **`peer auto <peerName>`**

<peerName>	The name of the peer server.

peer down

Description: Sets peer down.

Command Format: **`peer down <peerName>`**

<peerName>	The name of the peer server.

peer list

Description: Lists peers.

Command Format: **`peer list`**

There are no arguments for this command.

peer up

Description: Sets peer up.

Command Format: **`peer up <peerName>`**

<peerName> The name of the peer server.

radius client

Description: This command lists the client radius.

Command Format: **`radius clients`**

There are no arguments for this command.

server

This command manages server functions, such as server version.

Command Format: `server pause|resume|status`

The following section lists the **server** commands and their arguments:

server kill

Description: forcibly terminates the server without any warning.

Command Format: **`server kill`**

There are no arguments for this command.

server pause

Description: Pauses server.

Command Format: **`server pause`**

There are no arguments for this command.

server property add

Description: Adds a server property.

Command Format: **`server property add <name> = <value>`**

<name> The name of the server property.

<value> The value for the server property.

server property list

Description: Lists server properties.

Command Format: **`server property list`**

There are no arguments for this command.

server property set

Description: Sets a server property.

Command Format: **server property set <name> = <value>**

<*name*>	The name of the server property to be set.
<*value*>	The value of the server property to be set.

server property unset

Description: Unsets a server property.

Command Format: **server property unset <name>**

<*name*>	The name of the server property to be unset.

server resume

Description: Resumes server.

Command Format: **server resume**

There are no arguments for this command.

server shutdown

Description: Performs an orderly server shutdown.

Command Format: **server shutdown**

There are no arguments for this command.

server status

Description: Displays the server status.

Command Format: **server status**

There are no arguments for this command.

Example:

```
==> server status

server active
==>
```

server uptime

Description: Displays the server uptime.

Command Format: **server uptime**

There are no arguments for this command.

server version

Description: Displays the server version.

Command Format: **`server version`**

There are no arguments for this command.

session

This command manages session functions.

Command Format: **`session exec | info`**

The following section lists the **session** commands and their arguments:

session exec

Description: Executes a script file on this session.

Command Format: **`session exec <filename>`**

<filename>	The name of the script file.

session info

Description: Lists information about this session.

Command Format: **`session info`**

There are no arguments for this command.

stat

This command displays output statistics variable.

Description: Displays output statistics variable.

Command Format: **`stat <variable> [<ipAddress>]`**

<variable>	The statistics MIB variable from the RADIUS statistics.
[<ipAddress>]	The IP address of the client from which to request statistics.

stats

This command prints statistics associated with RADIUS MIBs.

Command Format: **`stats [-reset | -client <address> | -server <address:port> | -clients | -servers]`**

The following section lists the stats commands and their arguments:

stats client

Description: Lists statistics for a client.

Command Format: **`stats client <ipAddress>`**

<ipAddress> The IP Address of the client.

stats clients

Description: Lists clients with statistics.

Command Format: **`stats clients`**

There are no arguments for this command.

stats group list

Description: Lists the statistics of the group.

Command Format: **`stats group list`**

There are no arguments for this command.

stats inst list

Description: Lists instances of a group.

Command Format: **`stats inst list <group>`**

<group> Name of the group.

stats list

Description: Prints the statistics associated with RADIUS MIBs.

Command Format: **`stats list`**

There are no arguments for this command.

stats reset

Description: Resets the statistics.

Command Format: **`stats reset`**

There are no arguments for this command.

stats server

Description: Lists statistics for a server.

Command Format: **`stats server <ipAddress>`**

<ipAddress> Specifies the IP Address of the server.

stats servers

Description: Lists servers with statistics.

Command Format: **`stats servers`**

There are no arguments for this command.

stats var dump

Description: Lists the variables of a group.

Command Format: **`stats var dump <group>`**

`<group>` Name of the group.

stats var list

Description: Lists the variables of a group.

Command Format: **`stats var list <group>`**

<group> Name of the group.

system

This command displays a list of system properties.

Command Format: **`system [PROPERTY]`**

The following section lists the **system** commands and their arguments:

system hostaddr

Description: Lists IP address of this host.

Command Format: **`system hostaddr`**

There are no arguments for this command.

system hostname

Description: Lists FQDN of this host.

Command Format: **`system hostname`**

There are no arguments for this command.

system time

Description: Displays output current time.

Command Format: **`system time`**

There are no arguments for this command.

system version

Description: Displays output OS version.

Command Format: **`system version`**

There are no arguments for this command.

tacacsplus clients

This command displays a list TACACS+ clients

Command Format: **`system [PROPERTY]`**

There are no arguments for this command.

uss

The following section lists the **Universal State Server** (USS) commands and their arguments:

uss counts

Description: Displays output counter information.

Command Format: **`uss counts [<counter> [<attribute>]`**

[<counter> [<attribute>=]	The name of the counter from which information is retrieved.

uss entry

Description: Lists a state database entry.

Command Format: **`uss entry <key> [key | mod |ev |state |complete | attrs]`**

<key>	The IP address and port of the entry to retrieve.
[key | mod |ev |state |complete | attrs]	Specifies the field to get out of the database entry. If **`[key]`** is specified, as **`state entry key`**, all entries will be listed. However, if key and any other entry **(`mod, ev, state, compete, attrs`)** is specified, only that entry would be listed. For example: **`state entry [key | mod |`** would list only the mod entries.

uss index list

Description: Lists entries using index

Command Format: **`uss index list [<index>[<value>]]`**

<index>	This parameter specifies the name of the index to retrieve.
<value>	This parameter specifies the value for the index key.

uss keys

Description: Lists the keys.

Command Format: **`uss keys [<NASKeys>]`**

[<NASKeys>]	Specifies IP address of the entry to be retrieved.

uss list

Description: Lists a state entry.

Command Format: `uss keys [<Key>]`

[<Key>]	Specifies the IP address of the entry to be retrieved.

uss load

Description: Restores a state database from a file.

Command Format: **`uss load <fileName>]`**

[<fileName>]	The name of the file to be restored.

uss naslist

Description: Lists the NASs.

Command Format: **`uss naslist`**

There are no arguments for this command.

uss save

Description: Saves the state database to a file.

Command Format: **uss save <fileName>**

[*<fileName>]* The name of the file to which the state database will be saved.

Example*:*
```
==> uss save <filename>
Ok.
==>
```

uss stats

Description: Lists state database statistics.

Command Format: **uss stats <name>**

[<fileName>] The name of the file from which the database statistics will be extracted.

uss stats help

Description: Describes the state database statistics.

Command Format: **uss stats help**

There are no arguments for this command.

uss stats reset

Description: Resets state database statistics.

Command Format: **state stats reset**

There are no arguments for this command.

uss status

Description: Displays the state server replication state.

Command Format: **uss status**

There are no arguments for this command.

uss stop all

Description: Displays the state server replication state.

Command Format: **uss stop all**

There are no arguments for this command.

uss stop key

Description: Stops a state entry by key.

Command Format: **`uss stop key <key>`**

`<key>`	The key associated with the state entry to be stopped.

uss stop nas

Description: Stops all entries for a NAS.

Command Format: **`uss stop nas`**

There are no arguments for this command.

uss2 entry dump

Description: Displays selected or all data from one or all the entries.

Command Format: **`uss2 entry dump <model> [<key>] [<key|naskey|state|sessionid|mod|ev|attrs>]`**

<model>	Name of the model
<key>	The key associated with the state entry to be displayed.
<key|naskey|state|sessionid|mod|ev|attrs>	Specifies the field to get out of the database entry. If `[key]` is specified, as `state entry key`, all entries will be listed. However, if key and any other entry (`mod, ev, nas, state,attrs`) is specified, only that entry would be listed. For example: `state entry [key | mod |` would list only the mod entries.

uss2 entry list

Description: Displays entry data from one or all entries.

Command Format: ***`uss2 entry list <model> [<key>] ]`***

<model>	Name of the model.
<key>	The key associated with the state entry to be displayed.

uss2 load

Description: Reloads session state from the given file.

Command Format: **uss2 entry list <model> [<file>]]**

<model> Name of the model

<file> The file name.

uss2 model dump

Description: Displays information about one or all models.

Command Format: **uss2 model dump <model-name>]**

<model-name> Name of the model.

uss2 model stats

Description: Displays global statistics for the given model.

Command Format: **uss2 model stats <model-name>]**

<model-name> Name of the model.

uss2 node list

Description: Displays one or all nodes.

Command Format: **uss2 node list [<node-name>]]**

<node-name> Name of the node.

uss2 node stats

Description: Displays statistics of one or all nodes.

Command Format: **uss2 node stats [<node-name>]]**

<node-name> Name of the node.

uss2 repl stats

Description: Displays replication statistics for one or all nodes.

Command Format: **uss2 repl stats [<node-name>]]**

<node-name> Name of the node.

uss2 reset

Description: Resets the given session.

Command Format: **uss2 reset <model> <key>**

<model>	Name of the model
<key>	The key associated with the state entry to be reset.

uss2 reset all

Description: Resets all the sessions in the model.

Command Format: **uss2 reset all<model>**

<model>	Name of the model.

uss2 reset nas

Description: Resets all the sessions for a given NAS.

Command Format: **uss2 reset nas <model> <nas-key>**

<model>	Name of the model.
<nas-key>	The key associated with NAS.

uss2 resources

Description: Displays the available resources.

Command Format: **uss2 resource**

There are no arguments for this command.

uss2 resource dump

Description: Displays selected or all data from one or all resources.

Command Format: **uss2 resource dump <model> [<name>] [<value>]**

<model>	Name of the model.
<name>	Name of the resource.
<value>	Value of the resource.

uss2 resource list

Description: Displays information about one or all resources.

Command Format: **uss2 resource list <model> <resource> [<name>]**

<model>	Name of the model.
<resource>	Resource type.
<name>	Name of the resource.

uss2 save

Description: Saves all session state to thgiven file.

Command Format: **uss2 save <model> [<file>]**

<*model*>	Name of the model.
<*file*>	Name of the file.

END OF STEPS

Part VIII: Appendix

Overview

Purpose

This part contains the Appendix chapter(s) related to SMT.

Contents

This part includes the following chapter(s).

A Supplementary Information

Overview

Purpose

This section provides additional material to supplement the subject matter of the manual.

The following topics are included in this chapter:

Displaying the Built-in Web Interface

About Displaying the Built-in Web Interface

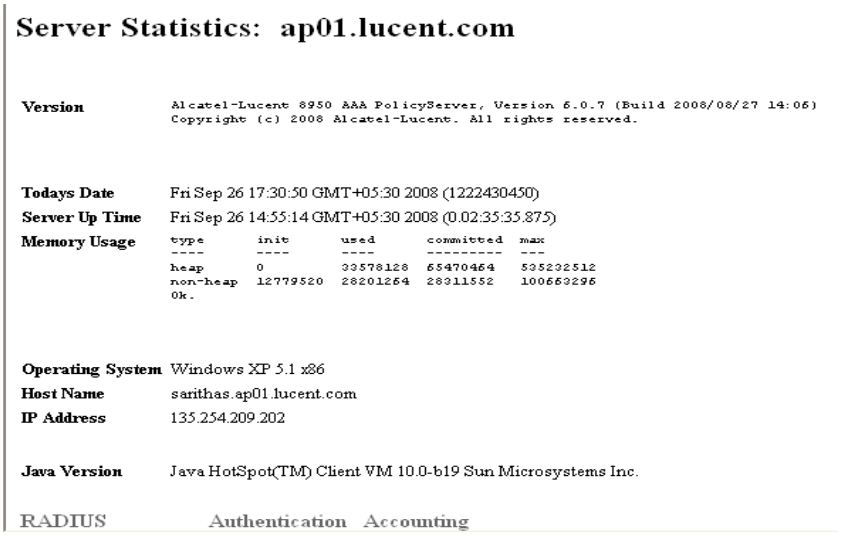
To display the built-in Web interface, perform the following procedure:

1. Open a browser window.
2. Using the IP address of the 8950 AAA server, set the URL field to the following:
   `http://IP address:9080`

   Result: A login window appears.
3. Enter the login and password

   Result: The Web interface appears as shown in Figure A-1.

Figure A-1 Built-in Web Interface



Displaying the RADIUS Server Administration Interface

About RADIUS Server Administration Interface

Use the following procedure to display the RADIUS server Admin interface:

1. Using the IP address of the 8950 AAA server, open a Telnet window using the following command:

   `telnet IP address 9023`

   Result: A Telnet screen appears.

2. Using the administrator username and password, enter the following command:

   `login username password`

3. At the prompt, enter **`help`** to display a list of commands for the RADIUS server that may be used through this interface. Figure A-2 shows such a telnet session.

Figure A-2 Telnet Session Using RADIUS Server Administration Address

```
900 Login required.
???? ????'??????

900 Login required.
login admin admin
login admin admin
102 2 records.
Alcatel-Lucent 8950 AAA PolicyServer, Version 6.0.7 (Build 2008/08/27 14:06)
Copyright (c) 2008 Alcatel-Lucent. All rights reserved.
policy-sachinkc-c1> help
help
103 Multi-line response follows.
cache add                     - add an entry to a cache
cache count                   - count entries matching key (trailing wildcard ok)
cache delete                  - delete entries matching key (trailing wildcard ok)
cache dump                    - dump entries matching key (trailing wildcard ok)
cache list                    - list entries matching key (trailing wildcard ok)
cache load                    - load cache contents from a file
cache names                   - list cache names
cache save                    - save cache contents to a file
client classes                - list client classes
derby backup                  - Backup an internal derby database
derby connect                 - Connect to a Derby database
derby create                  - Create an internal derby database
derby disconnect              - Disconnect from a Derby database
derby exec                    - Execute an SQL statement against a connected database
derby freeze                  - Freeze an internal derby database
derby info                    - Lists some metadata for the currently open connection
derby list                    - Lists internal derby databases
derby login                   - Cache security credentials for Derby access
```

Displaying the Configuration Server Administration Interface

About Configuration Server Administration Interface

Use the following procedure to display the configuration server administration interface:

1. Using the IP address of the 8950 AAA server, open a Telnet window by executing the following command:

   `telnet IP address 9020`

   Result: A Telnet screen appears.

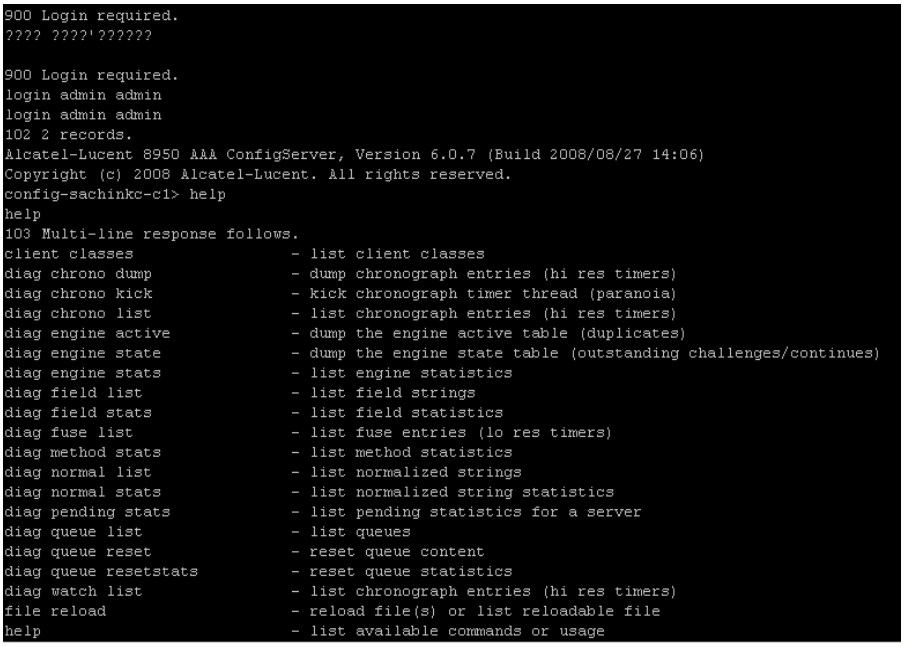
2. Using the administrator username and password, enter the following command:

   `login username password`

3. At the prompt, enter `help` to display a list of commands for the configuration server that may be used through this interface.

Figure A-3 shows such a telnet session.

Figure A-3 Telnet Session-Configuration Server Administration Address



Glossary

A

AAA
Authentication, Authorization, and Accounting

AAA SERVER
See RADIUS Server

ACCESS-ACCEPT
Authentication acknowledgement sent by the server to the client in response to an Access-Request signaling that local policy requirements have been met

ACCESS POINT
Hardware device or software that acts as a communication hub for users of a wireless device to connect to a wired LAN

ACCESS-REQUEST
A query or question sent from a client to the server that asks if the user is allowed to use the requested services and access the network

ACCOUNTING
Process of recording information about a user session

ACCOUNTING REQUEST
Request to the server for information in order to charge and track resource usage

ACCOUNTING START
An accounting request that has its accounting start attribute set to start

ACE/SERVER®
RSA product that acts as a server for a 8950 AAA server

APPLICATION
A collection of executable and configuration files that, when operated upon, provide a defined set of functionality

ATTRIBUTES
Information used for defining session parameters and available services

ATTRIBUTE SETS
Groups of verification attributes and reply attributes

ATTRIBUTE VALUE PAIR (AVP)
Combination of an attribute name and a value

AUTHENTICATION
Process of validating the user's identity

AUTHENTICATION KEY
A signature that identifies itself to the NAS to insure an additional layer of security

AUTHENTICATION REQUEST
This data packet identifies the NAS, the port used for connection, the user name, and the password. The password is encrypted to insure extra security.

AUTHENTICATION SOURCE
This term refers to two items that relate to password verification. It is the place where a user's password is stored, such as a user profile. It is also an external service that authenticates a user, such as a secure token server.

AUTHORIZATION
Process of validating that the user is allowed to do what was requested

B

BASE-NAME
A name assigned by a system administrator to a specific user account (See NAI and REALM)

C

CHAP
Challenge-Handshake Authentication Protocol

CGI
Common Gateway Interface—a means of transferring data between a Web server and a CGI application in order to interact with users

CHECK-ITEMS
Information that the server uses to determine how to respond to a RADIUS request (See VERIFICATION ATTRIBUTES)

CIDR
Classless Internet Domain Routing—A means to define a group of IP addresses using one IP address followed by a forward slash (/) and a number, such as 192.168.5.0/24

CLIENT
Application or machine that requests resources for its use from the server

COMMUNITY STRING
Character string that allows access to a database

CONFIGURATION SERVER
System that is used by the Server Managment Tool to collect server configuration information and statistical information regarding the 8950 AAA Server and the Universal State Server

CPU
Central Processing Unit

D

DIAMETER

An Authentication, Authorization, and Accounting (AAA) protocol.

DATA PACKET

Information transmitted over a network

DATA PANE

Part of the SMT GUI where each SMT panel is displayed

DNIS

Dialed Number Identification Service—Identifies the number that the caller dialed

E

EAP

Extensible Authentication Protocol—Protocol most commonly used in wireless LAN (Wi-Fi) applications

EDIT MENU

List of SMT commands that manage text, server preferences, and the use of data panes

F

FQDN

Fully Qualified Domain Name— Identifier such as *www.vitalaaa.com* which is comprised of a host (*www*) and domain name (*vitalaaa.com*). The domain name is further divided into a second-level domain (*vitalaaa*) and a top-level domain (*.com*).

G

GUI

Graphical User Interface, a means of running an application by using a mouse, point and click operations, and windowing components

H

HASH

Numeric value created from a text string

HELP MENU

List of SMT commands that control the Help Pane

HELP PANE

Part of the SMT GUI where help information is displayed

HTTP

HyperText Transfer Protocol—Protocol used by the World Wide Web

I

ISP
Internet Service Provider

ISDN
Integrated Services Digital Network

J

JDBC
Java Database Connectivity, an application programming interface (API) that allows Java programs to execute SQL statements

JDK
JAVA Development Kit

K

L

LDAP
Lightweight Directory Access Protocol - Protocol for accessing on-line directory services running over TCP/IP. LDAP provides the ability to locate resources within a network and make them available, whether on the Internet or a corporate intranet.

LDAP DIRECTORY
Authentication source used by LDAP directory service

LIMITED WILDCARD
Placing an asterisk (*) only at the beginning or end of a character string to perform pattern matching

LINUX
Free, open source operating system that runs on many different platforms, including PC and Macintosh

LISTENING ADDRESSES
Ports used for receiving authentication requests

LOG PANE
Part of the SMT GUI where log messages are displayed

M

MD5
Algorithm that creates digital signatures

MENU
List of commmands for an application accessible through a GUI

MESSAGE
Unit of transmission in a transport layer protocol

MESSAGE AUTHENTICATOR
Hashed version of a complete RADIUS message

METHOD
A programmed procedure that is executed when an object receives a message

MICROSOFT ACTIVE DIRECTORY
Windows 2000 directory service

N

NAI
Network Access Identifier — username (See BASE-NAME and REALM)

NAS
Network Access Server — Generic term for a network server that a user may access. After the user dials into the NAS, the NAS prompts the user for a user name and password. The user enters the information which the NAS receives.

NAVIGATION PANE
Part of the SMT GUI that contains a list of panel names used for displaying each SMT panel

NUL
A null character is a binary value with all its bits set to 0. It has a numeric value of 0. NULs can be used to mark the end of a character string or pad a data field.

O

P

PANE
Part of a window within a Graphical User Interface (GUI)

PANEL
GUI component comprised of other components or widgets, such as tabs, text fields, buttons, and panes

PANEL MENU
List of SMT commands that manage control of the active panel

PAP
Password Authentication Protocol

PASSWORD FILE
File located on a UNIX system using the directory paths */etc/passwd* or */etc/shadow*

PLATFORM
An integrated set of software components that form a base on which applications can be developed

PLUG-IN
A custom feature that can be added to an application without modifying the base code

POLICY
A set of rules that the server uses to determine access rights, user privileges, and accounting practices based on the user who is requesting access

POLICYASSISTANT
8950 AAA tool used for creating PolicyFlow

POLICYFLOW
A set of AAA decisions used for processing a RADIUS request

POP
Post Office Protocol, used for retrieving email from a mail server

PPP
Point-to-Point Protocol, used for connecting to the Internet

PROCESS
A program from disk combined with the OS overhead necessary to support its execution

PROTOCOL
Format used for transmitting data between two devices

PROXY SERVICE
A service that enables access requests to be forwarded to other servers—either directly or through intermediary servers—for authentication and, optionally, authorization

R

RADIUS
Acronym that stands for *Remote Authentication Dial-In User Services* See RADIUS SERVER

RADIUS DETAIL FILE
Text file used for storing session and billing data

RADIUS PROTOCOL
Special guidelines that define the information that must be passed in order to successfully access the destination system or service

RADIUS SERVER
A server that enables companies to authenticate, authorize, and account for remote users who request access to a network system or service

RADIUS USER FILE
A text file that conforms to a traditional format defined by the RADIUS protocol

READ COMMUNITY
Character string that allows access to a database in order to access read variables from the server

REALM
Part of the user-name used for grouping users who share the same domain. It is separated from the individual username by commercial at (@) or forward slash (/).

REMOTE METHOD INVOCATION (RMI)
Set of protocols that provide communication among Java objects

REPLY ATTRIBUTES
Information that the server returns to the client to configure the session

REPLY-ITEMS
See REPLY ATTRIBUTES

REPORTS MENU
List of SMT commands that manage printed or displayed output

ROOT USER
System administrator specified during installation of 8950 AAA.

S

SAFEWORD SERVER
Product of Secure Computing that communicates with 8950 AAA servers

SAM
See WINDOWS SAM

SERVER
Computer or device that manages network resources, for example, the UNIX host machine that contains 8950 AAA and supporting software

SERVER MANAGEMENT TOOL
8950 AAA application used for configuring and managing 8950 AAA servers

SERVER MENU
List of SMT commands that manage server connections

SHARED SECRET
A character string specified on both a server and another device or server that establishes mutual identification. A shared secret is required for proxy or remote servers. The shared secret is used to encrypt the user's password so it does not travel acrosss the network in clear text. The server in turn uses the shared secret to decrypt the password upon receipt.

SLIP
Serial Line Internet Protocol, used for connecting to the Internet through dial-up access

SMT
See Server Management Tool

SNMP
Simple Network management Protocol—Group of protocols used for large networks

SQL
Structured Query Language

SQL DATABASE
Structured Query Language database, the built-in database required by the PolicyAssistant

SYSTEM OPERATOR
System administrator with access to SMT and other administrative interfaces

T

TCP/IP
Transmission Control Protocol/Internet Protocol. A transport protocol commonly used over a network. The 8950 AAA application currently supports TCP/IP only.

TECHNICAL SUPPORT FILE PACKAGER
SMT tool for selecting and sending server files to the 8950 AAA technical support team

TELNET
Terminal emulation program that makes a computer behave like a specific type of terminal

THREAD
A program component that can run independently

TIMEOUT
Amount of time to wait before an action is taken

TIMEOUT LINGER
Additional time beyond the timeout period before an action is taken

TNS LISTENER
The TNS Listener is a persistent daemon process, run by Oracle that “listens” to the 8950 AAA application for database commands and updates.

TOOLBAR
Row of buttons used for invoking commands to a GUI-based application

U

UI
User Interface application. This application is responsible for providing each 8950 AAA Server Management Tool user with a graphic interface to communicate with 8950 AAA.

UNIX
This is one of the Operating Systems that provides an environment to govern how resources are used on the machine. Such resources include CPU, RAM memory, and secondary storage. UNIX also supports the execution of user-level programs.

USER PROFILE
Information about a specific user used by the server for processing requests.

USER SOURCE
Location where user profiles are maintained, such as a file, database, or a directory

USS
Universal State Server—In-memory database optimized to track network resource usage

V

VERIFICATION ATTRIBUTES
Information that the server uses to determine how to respond to a RADIUS request (See CHECK-ITEMS)

W

WI-FI
Wireless Fidelity, wa term that refers to any type of 802.11 network

WINDOW MENU
List of SMT commands that manage SMT panels

WINDOWS SAM
Windows Security Accounts Manager, a user source supported by 8950 AAA

WRITE COMMUNITY
Character string that allows access to a database in order to access write variables from the server

X

Y

Z

Index